Política de Classificação da Informação

Controle de Versões

Versão	Data	Autor	Notas da Revisão
1.0	01/10/2020	Airton Coelho	Versão Inicial
1.1	20/10/2020	Airton Coelho	Revisão
1.2	20/11/2020	Airton Coelho	Revisão
1.3	10/08/2021	Airton Coelho	Revisão LGPD
1.4	10/10/2025	Airton Coelho	Revisão

Sumário

CONTROLE DE VERSÕES 2

1. OBJETIVO 3

2. ESCOPO E APLICABILIDADE 3

3. REFERÊNCIAS 3

4. PRINCÍPIOS 3

5. DEFINIÇÕES 3

6. RESPONSABILIDADES PELA CLASSIFICAÇÃO E REVISÃO 4

6.1. Responsabilidades Gerais 4
6.2. Responsabilidades dos Usuários das Informações 5
6.3. Responsabilidades dos Cargos de Chefia 5
6.4. Responsabilidades dos Prestadores de Serviço 6

7. GESTÃO E TRATAMENTO DA INFORMAÇÃO 6

7.1. Direito de Propriedade 6
7.2. Direito de Acesso 7
7.3. Classificação da Informação 7
7.3.1. Classificação e Proteção de Informações Relativas a Crianças e Adolescentes 8
7.4. Tratamento Conforme Classificação 9
7.5. Requisitos Gerais de Rotulagem 13
7.6. Requisitos Específicos Para os Serviços de Nuvem 14
7.6.1. Controles Mínimos Obrigatórios para Ativos Restritos e Confidenciais em Nuvem 14
7.6.2. Responsabilidade Compartilhada 15

8. SANÇÕES 15

8.1. Solicitação e Autorização de Exceções 15

1. OBJETIVO

Estabelecer diretrizes e requisitos para classificar, proteger, armazenar, transmitir, rotular, reter e eliminar as Informações sob responsabilidade da FUTURE, garantindo proteção adequada de acordo com seu nível de criticidade, valor estratégico, sigilo e requisitos legais, com requisitos específicos para ambientes em nuvem e tratamento de Dados Pessoais (PII), em conformidade com a LGPD e com as normas ISO/IEC 27001, 27701, 27017 e 27018.

2. ESCOPO E APLICABILIDADE

Esta política aplica-se a todos os colaboradores, prestadores de serviço, parceiros, fornecedores, visitantes e terceiros que criem, acessem, processem, armazenem ou transmitam Informações em nome da FUTURE, incluindo subsidiárias e operações em quaisquer jurisdições onde a organização atue. Aplica-se a ativos físicos e digitais, bem como a serviços em nuvem (SaaS, PaaS, IaaS).

3. REFERÊNCIAS

- Normas ISO/IEC 27001, 27002, 27701, 27017, 27018.
- Lei Federal Nº 13.709/2018 (LGPD).
- Política de Segurança da Informação da Future.
- Contratos e Acordos com Fornecedores.

4. PRINCÍPIOS

A proteção das informações na Empresa é guiada pelos seguintes princípios fundamentais:

I. a proteção dos ativos de informação como elemento estratégico para a continuidade, competitividade e reputação da FUTURE;

II. a responsabilidade da alta administração e das áreas gestoras na definição de diretrizes, priorização de recursos e promoção de ambiente organizacional que assegure práticas adequadas de segurança da informação;

III. a garantia dos direitos dos titulares de dados pessoais, assegurando tratamento lícito, transparente e aderente às bases legais da LGPD, bem como o respeito à privacidade e às hipóteses legais de sigilo;

IV. a educação, conscientização e capacitação contínua como instrumentos essenciais para o fortalecimento da cultura de segurança da informação entre colaboradores, fornecedores e parceiros;

V. a gestão de riscos como fundamento para a definição de controles e medidas de proteção, considerando vulnerabilidades, ameaças, impactos ao negócio e requisitos legais;

VI. a confidencialidade, integridade e disponibilidade da informação como pilares para manutenção de ambientes confiáveis, acessíveis, íntegros e protegidos contra acessos, alterações ou indisponibilidades não autorizadas.

5. DEFINIÇÕES

Para fins desta Política de Classificação da Informação, aplicam-se as seguintes definições:

I. **Ambiente em nuvem**: Infraestrutura, plataforma ou serviço de software disponibilizado por terceiros (IaaS, PaaS ou SaaS) para armazenamento, processamento, hospedagem ou disponibilização de informações, devendo ser utilizado em conformidade com critérios de segurança, confidencialidade e localização dos dados estabelecidos pela FUTURE.

II. **Classificação da Informação:** Processo de categorização das informações conforme sua sensibilidade, criticidade e impacto potencial em caso de divulgação, alteração ou perda.

III. **Controlador**: Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

IV. **Dados Pessoais** (PII): Qualquer informação que permita identificar uma pessoa natural (pessoa física). Incluem-se dados como nome, CPF, endereço, dados de contato, registros eletrônicos, entre outros que permitam a identificação direta ou indireta do indivíduo.

V. **DPA (Data Processing Agreement)**: Instrumento contratual que estabelece obrigações, limites, responsabilidades, controles e medidas de segurança relacionadas ao tratamento de dados pessoais entre o Controlador e o Operador, ou entre operadores que compartilhem dados entre si.

VI. **Encarregado de Dados / DPO**: Pessoa indicada pela FUTURE para atuar como canal de comunicação entre a FUTURE, os titulares dos dados pessoais e a Agência Nacional de Proteção de Dados (ANPD), conforme previsto no art. 41 da LGPD.

VII. **Informação / Ativo de Informação**: Representa qualquer dado, registro, documento, conhecimento, material, sistema, plataforma, mídia ou recurso que possua valor para a FUTURE, independentemente do formato (físico, digital, oral ou visual) ou do meio de armazenamento.

VIII. **Operador**: Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

IX. **Proprietário da Informação:** Gestor responsável pelo ativo de informação, normalmente associado à área que a cria ou utiliza como insumo principal. Compete a ele definir sua classificação, revisar sua atualização e assegurar que o tratamento realizado esteja conforme esta Política.

X. **Prova de Eliminação (Proof of Destruction):** Evidência documental ou eletrônica que comprova a exclusão definitiva de informações ou dados pessoais, de forma que não possam ser recuperados ou reconstruídos, aplicável especialmente a procedimentos de descarte seguro.

XI. **Usuário / Custodiante da Informação:** Pessoa que utiliza ou manipula a informação no desempenho de suas atividades. É responsável por cumprir os controles de segurança, guardar a confidencialidade e reportar eventuais incidentes.

6. RESPONSABILIDADES PELA CLASSIFICAÇÃO E REVISÃO

6.1. Responsabilidades Gerais

a) O proprietário da informação (gestor da área que a cria, mantém ou utiliza como insumo principal) é responsável por definir sua classificação, revisar periodicamente sua adequação e garantir que o tratamento da informação esteja alinhado a esta Política;

b) Cada área é responsável pelos ativos de informação sob sua guarda, devendo assegurar sua proteção e uso adequado, observando a classificação atribuída e aplicando os controles correspondentes;

c) O Encarregado de Proteção de Dados, sempre que solicitado, deverá apoiar os departamentos no processo de classificação, reclassificação e tratamento de informações categorizadas como dados pessoais;

d) Todos os usuários devem observar o princípio do menor privilégio, utilizando, acessando e compartilhando informações estritamente dentro das permissões atribuídas a seu papel funcional. A Gestão de Identidades e Acessos (IAM) é responsável por assegurar que os controles de acesso estejam alinhados ao nível de classificação.

e) Qualquer alteração de finalidade, sensibilidade, contexto de uso, novo compartilhamento ou migração de ambiente (ex.: para nuvem, terceiros ou sistema externo) exige **reavaliação da classificação** antes da continuidade do tratamento;

f) Qualquer departamento poderá propor a alteração da classificação de determinada informação, sempre que houver mudança de uso, sensibilidade, risco ou valor do ativo. A alteração será avaliada e aprovada pelo responsável pelo CTO (Chief Technology Officer) da FUTURE e, quando envolver dados pessoais, pelo Encarregado de Proteção de Dados.

6.2. Responsabilidades dos Usuários das Informações

Os usuários que acessam, manipulam ou armazenam informações da FUTURE devem:

a) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

b) Cumprir integralmente esta Política e demais normas de segurança da informação, sob pena de incorrer em sanções disciplinares e legais cabíveis;

c) Utilizar os sistemas de informações da FUTURE e os recursos a ela relacionados somente para os fins previstos pelas Políticas da empresa;

d) Adotar as medidas de proteção específicas definidas para os ativos de informação sob seu uso ou responsabilidade;

e) Manter sigilo sobre suas credenciais de acesso aos recursos e sistemas da FUTURE, sendo expressamente vedado seu compartilhamento.;

f) Não divulgar, compartilhar ou disponibilizar informações classificadas a terceiros não autorizados, independentemente do meio utilizado;

g) Comunicar, imediatamente, ao Encarregado de Proteção de Dados ou ao CTO qualquer suspeita de incidente, irregularidade ou conduta que viole esta Política.

6.3. Responsabilidades dos Cargos de Chefia

A responsabilidade das chefias compreende, dentre outras, as seguintes atividades:

a) Assegurar que seus subordinados, parceiros e prestadores de serviço cumpram esta Política e as demais normas de segurança da informação;

b) Identificar os desvios praticados e adotar as medidas corretivas apropriadas à gravidade da ocorrência;

c) Garantir a imediata revogação dos acessos de funcionários desligados, transferidos ou afastados, seguindo os procedimentos formais estabelecidos pelo respectivo plano de desligamento do funcionário;

d) Proteger, no nível físico e lógico, os ativos de informação e de processamento da FUTURE relacionados com a sua área de atuação;

e) Garantir que seus subordinados recebam orientação necessárias para cumprir sua obrigação de proteger as informações da FUTURE;

f) Comunicar formalmente à área de Segurança da Informação e ao Encarregado de Proteção de Dados quais funcionários e prestadores de serviço, sob sua supervisão, podem acessar as informações da FUTURE, seguindo as normas de classificação de informações e os perfis de cada cargo, observado o princípio do menor privilégio.

g) Difundir e reforçar a seus subordinados, de forma contínua, as responsabilidades previstas neste documento.

6.4. Responsabilidades dos Prestadores de Serviço

Prestadores de serviço que acessam, manipulam ou armazenam informações da FUTURE estão sujeitos às mesmas diretrizes e responsabilidades aplicáveis aos colaboradores internos no que diz respeito à proteção e ao tratamento adequado das informações classificadas. Além disso:

a) Os contratos firmados com prestadores de serviço devem conter cláusulas específicas que estabeleçam a obrigação de cumprimento desta Política, incluindo requisitos de confidencialidade, proteção de dados pessoais, segurança da informação e penalidades por descumprimento;

b) Prestadores e terceiros devem tratar as informações da FUTURE com o mesmo nível de proteção exigido aos colaboradores internos, respeitando classificações, controles de acesso e orientações recebidas;

c) Quando houver tratamento de dados pessoais, o prestador deve aderir às diretrizes legais aplicáveis, bem como ao DPA (Data Processing Agreement) firmado com a FUTURE, assegurando o cumprimento das obrigações previstas na LGPD.

7. GESTÃO E TRATAMENTO DA INFORMAÇÃO

7.1. Direito de Propriedade

As informações produzidas, recebidas, tratadas ou armazenadas no âmbito da FUTURE, em quaisquer meios ou formatos, constituem ativos de informação de propriedade exclusiva da empresa, devendo ser preservadas, protegidas e utilizadas exclusivamente para fins institucionais, em conformidade com esta Política e demais normas internas.

Somente nas seguintes condições a FUTURE poderá não deter a integralidade dos direitos sobre uma informação:

a) Quando houver previsão expressa em instrumento legal, contratual ou de propriedade intelectual, incluindo menção específica em copyright, licenciamento ou instrumento equivalente; ou

b) Quando a informação já tiver sido oficialmente tornada pública pela própria FUTURE, por meio de canais de divulgação previamente autorizados, incluindo websites, mídias institucionais, comunicados oficiais e materiais de imprensa.

A divulgação externa de informações classificadas, total ou parcialmente, só poderá ocorrer mediante autorização formal da Diretoria, observando-se os seguintes requisitos:

I. utilização dos canais oficiais de comunicação definidos pela FUTURE;

II. respeito às classificações de informação e aos controles de confidencialidade aplicáveis;

III. quando envolver dados pessoais, observância das diretrizes impostas pela LGPD e as orientações advindas do Encarregado de Proteção de Dados.

Qualquer divulgação indevida — acidental ou intencional — constitui violação desta Política e poderá resultar em medidas disciplinares, cíveis, contratuais e/ou penais.

7.2. Direito de Acesso

O acesso às informações da FUTURE deve ocorrer exclusivamente conforme a necessidade, seja por exercício funcional (no caso de colaboradores), seja por necessidade de negócio (no caso de clientes, fornecedores ou parceiros). É proibido acessar, consultar, modificar, copiar, armazenar ou transmitir informações além do estritamente necessário ao desempenho das atividades autorizadas.

A concessão e o uso do acesso são disciplinados por normas internas e instrumentos de responsabilização, conforme segue:

a) **Funcionários da FUTURE:** o acesso é concedido com base em necessidade funcional e/ou operacional, condicionado à assinatura de **Termo de Confidencialidade e Sigilo**, garantindo a proteção e o uso adequado das informações.

b) **Parceiros de negócio, fornecedores ou visitantes:** o acesso a informações ou instalações se dá apenas mediante assinatura do **Termo de Confidencialidade – Parceiros de Negócio**, assegurando a proteção jurídica das informações compartilhadas.

c) **Funcionários de organizações externas (prestadores de serviço terceirizados):** o acesso deve estar vinculado a cláusulas específicas de confidencialidade e preservação de sigilo (**Termo de Confidencialidade – Empresa** ou disposições contratuais equivalentes), incluindo a previsão de penalidades em caso de violação.

7.3. Classificação da Informação

A classificação das informações visa garantir que cada ativo informacional receba o nível adequado de proteção, conforme sua sensibilidade, valor para o negócio e impacto potencial decorrente de uso indevido, acesso não autorizado, alteração ou destruição.

Toda informação criada, recebida, processada ou armazenada pela FUTURE deve ser classificada em uma das categorias abaixo, considerando-se adicionalmente se contém dados pessoais, nos termos da Lei Geral de Proteção de Dados (LGPD):

a) **Pública:** Informações cujo acesso é livre ao público interno ou externo. Normalmente já se encontram divulgadas oficialmente ou são, por natureza ou determinação legal, de domínio público.

Exemplos: Política da Qualidade, Política de Segurança da Informação, materiais institucionais, publicações oficiais e conteúdos divulgados em mídias sociais.

b) **Interna:** Informações destinadas ao uso interno da FUTURE. Sua divulgação a terceiros pode expor processos internos, práticas operacionais ou estrutura organizacional.

Exemplos Manuais internos, procedimentos operacionais, instruções de trabalho, roteiros internos de atendimento.

c) **Interna / LGPD:** Informações internas que contêm dados pessoais. Além da classificação interna, devem observar os princípios, bases legais, finalidades e salvaguardas previstos na LGPD.

Exemplos: Listas internas contendo nomes, e-mails corporativos, dados cadastrais de colaboradores ou clientes para uso operacional.

d) **Restrito:** Informações sensíveis ou estratégicas, cujo acesso deve ser limitado a grupos específicos. A divulgação indevida pode gerar prejuízos financeiros, competitivos ou reputacionais.

Exemplos: Planejamento financeiro, estratégias comerciais, listas de prospecção, condições comerciais em negociação.

e) **Restrito / LGPD:** Informações restritas que envolvem dados pessoais, podendo causar impacto significativo tanto ao titular quanto à FUTURE em caso de exposição.

Exemplos: Dossiês de funcionários, dados de clientes vinculados a operações financeiras ou contratuais, históricos de relacionamento.

f) **Confidencial:** Informações críticas e de alto impacto para a continuidade e segurança da FUTURE. Exigem controles rigorosos de armazenamento, acesso e transmissão. A violação pode comprometer a operação, a segurança ou a posição estratégica da organização.

Exemplo: Chaves criptográficas, senhas administrativas, relatórios de vulnerabilidades, informações de segurança cibernética.

g) **Confidencial / LGPD:** Informações confidenciais contendo dados pessoais, cujo uso ou divulgação indevida pode gerar danos graves ao titular e à FUTURE, incluindo riscos legais, regulatórios e de imagem.

Exemplos: Registros sensíveis relacionados à saúde de colaboradores, relatórios investigativos internos envolvendo dados pessoais, informações pessoais vinculadas a incidentes de segurança.

7.3.1. Classificação e Proteção de Informações Relativas a Crianças e Adolescentes

Informações que contenham dados pessoais de crianças ou adolescentes devem receber atenção especial, em razão de seu caráter sensível e da necessidade de proteção reforçada prevista na legislação aplicável.

Esses dados **devem ser classificados, no mínimo, como "Restrita / LGPD"**, independentemente do contexto ou volume de informações envolvido.

Quando o conteúdo puder causar impacto elevado ao titular ou à FUTURE em caso de exposição (por exemplo, informações de saúde, benefícios médicos ou situações familiares), a classificação **"Confidencial / LGPD"** deve ser aplicada.

O acesso a essas informações deve ser limitado exclusivamente aos colaboradores que necessitem delas para desempenhar suas funções, mediante controle formal de permissões. Documentos, sistemas, relatórios, comunicações internas ou repositórios que contenham esse tipo de dado devem estar rotulados de forma clara e armazenados em ambientes seguros, com rastreabilidade de acesso e proteção contra compartilhamento indevido.

A retenção deve respeitar os prazos legais aplicáveis e, ao final, o descarte deve ser realizado de forma segura, garantindo que os dados não possam ser reconstruídos ou recuperados.

7.4. Tratamento Conforme Classificação

O tratamento das informações deve observar o nível de classificação atribuído e as medidas de proteção correspondentes.

Em caso de dúvida quanto à classificação apropriada de uma informação, esta deverá ser tratada, por padrão, como Restrita, até que a área proprietária confirme sua classificação definitiva.

Sempre que a informação contiver **dados pessoais**, a classificação receberá o sufixo **/LGPD** (ex.: "Interna / LGPD"; "Restrito / LGPD" e "Confidencial / LGPD"), devendo ser aplicados, adicionalmente, os requisitos de proteção de dados pessoais, tais como minimização, base legal, finalidade, registro das operações de tratamento e segurança adequada ao risco.

a) Pública

ATIVIDADE	DIRETRIZ
Acesso	Livre, sem restrições.
Divulgação	Permitida interna e externamente, sem autorização prévia.
Armazenamento	Pode ser armazenada em repositórios comuns, sem controle especial.
Transporte	Não exige medidas adicionais de segurança.
Descarte	Pode ser descartada sem procedimentos especiais.
Rotulagem	Não é obrigatória.

b) Interna e Interna / LGPD

ATIVIDADE	DIRETRIZ
Acesso	Somente funcionários e prestadores autorizados, conforme necessidade funcional.
Divulgação	Restrita ao ambiente interno, tanto para funcionários quanto para prestadores autorizados. É proibida a divulgação a familiares, amigos ou terceiros.
Armazenamento	**Informações na rede:** • Bloquear a estação de trabalho sempre que não estiver sob supervisão direta; • Não utilizar equipamentos ou credenciais de outro usuário, nem permitir o compartilhamento de contas;

ATIVIDADE	DIRETRIZ
	• Armazenar a informação em diretórios corporativos, preferencialmente com controle de permissões. **Documentos:** • Guardá-los em ambiente controlado, sem que estejam a vista de terceiros; • Documentos físicos devem ser guardados em local não acessível ao público; • Identificar claramente a classificação do documento, para evitar manuseio ou divulgação indevida. Mídias • Guardá-las em ambiente controlado e protegidas do acesso de terceiros; • Criptografá-las de forma a proteger seus dados.
Transporte	Somente funcionários e prestadores autorizados podem ter acesso. Pessoas não vinculadas à FUTURE não devem, em qualquer hipótese, acessar tais informações. Eventuais autorizações excepcionais serão concedidas apenas nas condições previstas no item *Direito de Propriedade*, mediante autorização formal e registro adequado.
Descarte	Antes de ser descartado: • Os documentos devem ser picotados de modo que seu conteúdo fique incompreensível ou ilegível; • As mídias magnéticas devem ser inutilizadas (por destruição do seu conteúdo ou inutilizando-as fisicamente de maneira que não possam ser reconstituídas).
Rotulagem	A capa ou rodapé do documento devem estar rotuladas como **documento INTERNO** ou **INTERNO / LGPD**. Informações como tickets no sistema de serviço, CRM, e ferramentas que possuem controle de classificação próprio não precisam ser rotuladas. Se houver qualquer dúvida quanto a classificação da informação, ela deve ser tratada como **Restrita**.

c) Restrita e Restrita / LGPD

ATIVIDADE	DIRETRIZ
Acesso	Limitado a pessoas e grupos específicos, devidamente autorizados e registrados. Justificativa deve estar alinhada ao item Direito de Acesso.
Divulgação	Proibida a divulgação fora do grupo autorizado. Conversas externas (familiares, redes sociais, eventos, terceiros em geral) são proibidas, sob pena de sanções disciplinares, administrativas, cíveis e penais.
Armazenamento	O armazenamento desse tipo de informação deve observar cuidados rigorosos, de forma a preservar sua confidencialidade, integridade e disponibilidade. Devem ser adotadas, no mínimo, as seguintes práticas: **Informações na rede:** • Bloquear a estação de trabalho sempre que não estiver sob supervisão direta;

ATIVIDADE	DIRETRIZ
	• Não utilizar equipamentos ou credenciais de outro usuário, nem permitir o compartilhamento de contas; • Armazenar os arquivos exclusivamente nos diretórios corporativos destinados a esse fim, preferencialmente com controles de permissão. **Documentos:** • Manter em local seguro e trancado, como armários ou gaveteiros de acesso restrito; • Identificar claramente a classificação do documento, para evitar manuseio ou divulgação indevida; **Mídias:** • Armazenar em local seguro e trancado, de acesso controlado; • Utilizar criptografia ou outro mecanismo equivalente de proteção para impedir acesso indevido ao conteúdo.
Transporte	O transporte deve ser realizado em recipientes lacrados e sem identificação do conteúdo, de modo a evitar qualquer exposição durante o percurso. Considerando a sensibilidade e o valor dessas informações, é imprescindível assegurar que somente pessoas devidamente autorizadas tenham acesso ao material transportado, adotando controle e registro sempre que necessário.
Descarte	Antes do descarte, devem ser adotadas medidas que impeçam a recuperação do conteúdo: • Documentos físicos devem ser triturados de forma a torná-los ilegíveis ou irreconhecíveis. • Mídias magnéticas e demais suportes de armazenamento devem ser inutilizados, seja por destruição segura do conteúdo (quando possível e aprovada pela área de Segurança), seja por destruição física que impeça sua reconstrução e recuperação.
Rotulagem	A capa ou rodapé do documento devem estar rotuladas como **documento RESTRITO** ou **RESTRITO / LGPD**. Informações como tickets no sistema de serviço, CRM, e ferramentas que possuem controle de classificação próprio não precisam ser rotuladas, pois já tem controle definido unitariamente.

d) Confidencial e Confidencial / LGPD

ATIVIDADE	DIRETRIZ
Acesso	O acesso deve ser limitado ao menor número possível de pessoas, restrito apenas àquelas cuja função exija o uso direto dessas informações. Tais acessos devem ser formalmente autorizados, justificados e registrados, conforme o princípio do menor privilégio.

ATIVIDADE	DIRETRIZ
	O envio ou compartilhamento desse tipo de informação deve ser evitado. Quando indispensável, deve ocorrer exclusivamente por meios criptografados e protegidos, observando-se os controles e ferramentas corporativas aprovadas.
Divulgação	Não devem ser divulgadas sob nenhuma circunstância, salvo quando houver necessidade comprovada e estritamente relacionada às atividades do negócio. Nessas situações, a divulgação deverá ser previamente autorizada pela Diretoria ou pelo Encarregado de Proteção de Dados, conforme o caso, e acompanhada da formalização de Acordo de Confidencialidade que estabeleça expressamente as responsabilidades, obrigações e penalidades aplicáveis em caso de violação. Sempre que possível, após o compartilhamento autorizado de informações sensíveis, devem ser adotadas medidas de mitigação, como a troca imediata de senhas ou chaves de acesso utilizadas de forma temporária. É proibido discutir, comentar ou expor informações confidenciais fora do contexto profissional ou com pessoas não autorizadas, incluindo familiares, amigos ou terceiros. A divulgação indevida configura violação desta Política e está sujeita às sanções disciplinares, contratuais e legais cabíveis.
Armazenamento	Por se tratar de informações **críticas**, seu armazenamento deve observar o **nível máximo de proteção**, de forma a evitar acesso indevido, perda, alteração ou destruição não autorizada. **Informações na rede:** • Bloquear a estação de trabalho sempre que estiver sem supervisão; • Não utilizar a máquina ou realizar login utilizando credenciais de terceiros; • Armazenar as informações somente em diretórios designados para esse fim, empregando mecanismos adicionais de segurança, como criptografia e assinatura/identificação digital; • Manter cópia de segurança de certificados digitais, chaves criptográficas e demais elementos necessários à recuperação em situações de contingência. **Documentos:** • Armazenar em ambiente seguro e trancado (preferencialmente cofres) com registro de logs ou controle de acesso; • Guardar as chaves ou senhas de acesso ao local de armazenamento em condição igualmente segura e sob controle restrito. **Mídias** • Manter todo o conteúdo criptografado; • Armazenar as mídias em ambiente seguro e trancado (preferencialmente cofres) com registro de logs ou controle de acesso; • Guardar as chaves, chaves criptográficas ou senhas associadas em local seguro e restrito, não armazenando-as no mesmo local da mídia.

ATIVIDADE	DIRETRIZ
Transporte	O transporte desse tipo de informação deve ser realizado com recursos máximos de segurança, garantindo que seu conteúdo permaneça completamente protegido durante todo o percurso. As informações devem ser acondicionadas em recipientes ou embalagens lacradas e opacas, sem indicação externa de conteúdo, prevenindo exposição acidental. Todo o processo de transporte deve ser formalmente registrado, incluindo, no mínimo: • Data e horário da transferência; • Nome e identificação do responsável pelo transporte; • Destinatário autorizado; • Número de série, lacre ou identificação da embalagem. Devido ao elevado valor e sensibilidade dessas informações, o acesso ao material durante o transporte deve ser restrito exclusivamente a pessoas previamente autorizadas, sendo vedado o manuseio, abertura ou inspeção por terceiros não autorizados, independentemente da relação de confiança ou vínculo profissional.
Descarte	Antes do descarte, deve-se garantir que o conteúdo não possa ser recuperado ou reconstruído: • **Documentos físicos:** devem ser fragmentados por meio de picotamento ou método equivalente, de modo a torná-los ilegíveis e irrecuperáveis. • **Mídias magnéticas ou digitais:** devem ser inutilizadas por meio de destruição lógica (apagamento seguro/secure wipe) ou destruição física que impossibilite sua reconstituição. Procedimentos de destruição física ou lógica devem ser avaliados e aprovados previamente pela área de Segurança da Informação.
Rotulagem	A capa e o rodapé do documento devem estar rotulados como **documento CONFIDENCIAL** ou **CONFIDENCIAL / LGPD**. O acesso a seu conteúdo deve deixar claro que é uma informação privilegiada e confidencial.

7.5. Requisitos Gerais de Rotulagem

Toda informação (documento, arquivo, base de dados, bucket, registro ou outro ativo informacional) deve conter metadados ou tags que indiquem, no mínimo:

I. Classificação da informação;
II. Proprietário (responsável);
III. Data de criação; e
IV. Prazo ou política de retenção aplicável.

Nos **sistemas considerados críticos**, a rotulagem deve ser **obrigatória** e tecnicamente **imposta**. Esses sistemas devem implementar mecanismos que:

I. Impeçam a realização de operações que possam resultar em exposição indevida da informação (como compartilhamento público, download, replicação ou envio para terceiros) quando as tags estiverem ausentes, incorretas ou inconsistentes;
II. Apliquem controles automáticos de visibilidade e acesso com base na classificação definida;

III. Bloqueiem a exposição pública ou transferência externa da informação caso não exista rotulagem adequada.

7.6. Requisitos Específicos Para os Serviços de Nuvem

A utilização de serviços em nuvem está sujeita simultaneamente aos controles internos da FUTURE e às responsabilidades compartilhadas estabelecidas pelo provedor de serviços. A FUTURE deve compreender, documentar e revisar periodicamente o modelo de responsabilidade compartilhada aplicável a cada serviço contratado, assegurando que:

I. as obrigações de segurança da informação, proteção de dados pessoais e continuidade de negócios estejam claramente definidas entre FUTURE e o provedor;

II. os serviços sejam configurados de acordo com as práticas seguras recomendadas pelo provedor e pelas normas internas;

III. os recursos utilizados na nuvem sejam devidamente identificados, classificados conforme esta Política e rotulados quando aplicável (metadados/tags);

IV. existam controles de acesso baseados em identidade (IAM), com aplicação de privilégios mínimos, autenticação multifator (MFA) e segregação de ambientes (desenvolvimento, homologação e produção);

V. logs de acesso, uso e alterações de configuração sejam coletados, armazenados de forma íntegra e monitorados;

VI. as configurações críticas, tais como exposição pública de buckets, endpoints e APIs, sejam periodicamente auditadas e corrigidas quando necessário;

VII. quando houver tratamento de dados pessoais, sejam observados adicionalmente os requisitos legais e orientações do Encarregado de Proteção de Dados.

7.6.1. Controles Mínimos Obrigatórios para Ativos Restritos e Confidenciais em Nuvem

I. **Criptografia**: TLS para transporte; criptografia em repouso com algoritmos aprovados (ex.: AES-256); políticas de rotação de chaves. Preferência por *customer-managed keys* para dados Confidenciais/LGPD.

II. **Gestão de chaves**: uso de KMS/HSM; separação de funções; logs de uso de chaves.

III. **Identidade e Acesso**: IAM granular, princípio do menor privilégio, MFA obrigatória para contas privilegiadas; revisão periódica de permissões.

IV. **Configuração segura**: proibição de *storage* público; *hardening* de imagens; *scanning* automatizado de exposição (buckets públicos, regras de firewall).

V. **Logging e Monitoramento**: habilitar logs de acesso, API e auditoria; retenção definida; envio de logs a repositório controlado pela Future quando possível.

VI. **Backups e replicação**: criptografia de backups, localização e proteção equivalentes, testes periódicos de restauração.

VII. **Testes de segurança**: exigir evidências de pentests e varreduras, e direito de realizar testes com coordenação.

VIII. **Monitoramento de conformidade**: verificar e avaliar os relatórios (certificações ISO/SOC, resultados de auditoria, scan de vulnerabilidades).

7.6.2. Responsabilidade Compartilhada

Em cada contratação ou habilitação de serviço em nuvem, deve ser documentado formalmente o modelo de responsabilidade compartilhada aplicável, discriminando de maneira explícita quais controles e atividades são de responsabilidade do provedor; e quais são de responsabilidade da FUTURE.

Esse documento deve ser aprovado pela área responsável pela Segurança da Informação, incorporado ao projeto ou contrato correspondente e disponibilizado às equipes envolvidas, garantindo entendimento e aderência aos controles estabelecidos.

8. Sanções

O descumprimento das diretrizes estabelecidas nesta Política, bem como de normas complementares e procedimentos dela decorrentes, poderá resultar na aplicação de sanções disciplinares, conforme previsto na Política de Segurança da Informação, nos instrumentos contratuais aplicáveis, e na legislação vigente.

As penalidades poderão incluir advertências, suspensões, desligamento, encerramento de contrato e demais medidas administrativas ou legais cabíveis, sem prejuízo da apuração de responsabilidade civil e/ou criminal, quando aplicável.

8.1. Solicitação e Autorização de Exceções

Qualquer necessidade de adoção de procedimentos que se afastem das diretrizes estabelecidas nesta Política de Classificação da Informação deverá ser previamente justificada e submetida à autorização formal da Diretoria. Nos casos que envolvam tratamento de dados pessoais, a autorização deverá ocorrer com a orientação e validação do Encarregado de Proteção de Dados (DPO).

Qualquer prática que represente descumprimento desta Política **sem autorização prévia** será considerada **infração**, sujeitando o responsável às sanções previstas nesta Política e na legislação aplicável.

Airton Coelho Vieira Jr