



**DOURO CAPITAL GESTORA DE RECURSOS E INVESTIMENTOS LTDA.**

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

**Setembro/2022**



## 1. OBJETIVO

Esta Política de Segurança da Informação (“Política”) da **DOURO CAPITAL GESTORA DE RECURSOS E INVESTIMENTOS LTDA.** visa preservar a confidencialidade, integridade e disponibilidade das informações utilizadas no desempenho de suas atividades, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte.

## 2. ABRANGÊNCIA

Esta política abrange todos os Colaboradores e Visitantes que possuam acesso à rede da DOURO, à informações confidenciais, aos equipamentos computacionais ou ambientes controlados que necessitem de um login ou cartão de acesso, para que lhe sejam disponibilizados tais informações.

Terão acesso às Informações Confidenciais e ambientes controlados da DOURO, dentro dos limites definidos, os Colaboradores que concordarem com a política registrando o aceite através da assinatura do TERMO DE COMPROMISSO apresentado quando de sua admissão na DOURO. Este termo determina a adesão do profissional a todas as políticas e normas internas, incluindo esta política.

O uso indevido dos recursos, em desacordo com a política poderá implicar em advertência, suspensão e demissão a critério da direção da empresa.

## 3. CONCEITOS

Para efeitos da presente política, considera-se:

**Rede DOURO:** Abrange todos os sistemas, diretórios e Intranet disponibilizados aos Colaboradores da DOURO, conforme perfil de acesso definido.

**Software:** São todos os programas instalados nos computadores.

**Ambiente Lógico:** ambiente controlado, eletrônico, onde circulam e são armazenadas Informações Confidenciais, softwares e sistemas.

**Ambiente físico:** dependências físicas da DOURO.

**Usuário:** Colaborador ou Colaboradores que detenham acesso aos ambientes físico e lógico da DOURO para o desempenho de suas atividades.

**Equipamentos Computacionais:** São todos os equipamentos de propriedade da DOURO disponibilizados ao uso dos colaboradores, incluindo, mas não se limitando, aos desktops, notebooks, impressoras, equipamentos de vídeo conferências e digitalizadores.

**Informações Confidenciais:** São consideradas informações confidenciais, para os fins desta



Política, quaisquer informações consideradas não disponíveis ao público ou reservadas, dados, especificações técnicas, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, software e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela DOURO em decorrência do desempenho de suas atividades.

Colaborador ou Colaboradores: todos os prestadores de serviço da DOURO.

Prestadores de serviços: pessoa jurídica ou física que mantenha contrato de prestação de serviço, ou tenha celebrado instrumento afim com quaisquer das sociedades da DOURO.

Visitante: todo indivíduo que não mantenha qualquer sorte de vínculo formal com a DOURO, enfim, todos aqueles que não se enquadram na definição de Colaborador, conforme acima.

#### **4. RESPONSABILIDADES**

##### **DOURO:**

- Inclusão no planejamento orçamentário anual o valor de investimento em recursos computacionais, incluindo aquisição e renovação de equipamentos e softwares;
- Fornecer capacidade suficiente para realização dos Backups referentes aos processos e atividades da empresa;
- Fornecer espaço suficiente no SERVIDOR DE ARQUIVOS para armazenamento seguro de arquivos que contenham informações referentes aos processos e atividades da empresa.

##### **COLABORADORES:**

- Indicação de suas necessidades de recursos de TI;
- Utilização dos recursos de TI de acordo com o Código de Conduta da DOURO;
- Utilização da ferramenta de Correio Eletrônico para uso profissional;

#### **5. POLÍTICA DE CONFIDENCIALIDADE**

Neste item são definidas como serão tratadas as informações institucionais, forma de uso, possibilidade ou não de disponibilização ao ambiente externo ou a terceiros. Assim, sempre que houver a necessidade de utilização de informações de conteúdo institucional, é necessário atentar-se para as determinações abaixo descritas:

##### **5.1. PROPRIEDADE DAS INFORMAÇÕES E SOFTWARE**

Os dados e informações criados nos Recursos Computacionais da DOURO são de sua propriedade e devem ser utilizados pelos Colaboradores, Prestadores de Serviços e



Consultores, exclusivamente, no exercício de suas atividades junto à empresa. Os softwares adquiridos no mercado ou desenvolvidos internamente pertencem exclusivamente à DOURO, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas, elaboradas e/ou desenvolvidas pelos Colaboradores, durante a vigência da relação de emprego ou contrato, ou quando forem utilizados recursos, dados, meios, materiais, instalações, equipamentos, informações tecnológicas e segredos comerciais, pertencentes à DOURO, sendo vedada a cópia ou disponibilização através de qualquer meio (eletrônico ou físico) para ambiente externo à DOURO.

Toda estrutura mantida pela DOURO, composta pela rede, telefonia, correio eletrônico, internet e outros meios de comunicação, são instrumentos de trabalho de sua propriedade que o mesmo disponibiliza aos colaboradores a fim de tornar suas tarefas mais eficientes. Da mesma forma, todos os documentos, estejam eles em forma impressa ou eletrônica, ou que circulem por estes meios, também são de propriedade da DOURO e todos os Colaboradores devem envidar esforços para protegê-los do uso indevido. É proibido o uso destes documentos fora da DOURO cujo objetivo não seja atender, exclusivamente, aos interesses da instituição. Sua retirada ou envio com qualquer outra finalidade constitui violação a esta política. A sua transmissão via correio eletrônico, fax ou outro meio, deverá ser feita com o máximo de atenção. Os documentos alterados fora da DOURO devem ter seus arquivos ou na rede ou atualizados imediatamente.

## 5.2. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações que transitam pela DOURO são, para fins desta Política, classificadas em quatro padrões distintos, a saber:

**INFORMAÇÕES PÚBLICAS:** Aquelas destinadas a disseminação fora da DOURO. Possuem caráter informativo geral e são direcionadas a clientes. Exemplos: material de marketing, clipping information, registros regulamentares e da Comissão de Valores Mobiliários.

**INFORMAÇÕES INTERNAS:** São aquelas destinadas ao uso dentro da DOURO. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente a DOURO ou seus clientes e colaboradores. Essas informações não exigem proteções especiais salvo aquelas entendidas como mínimas para impedir a divulgação externa não intencional.

**INFORMAÇÕES CONFIDENCIAIS:** Também destinam-se a uso interno da DOURO. Entretanto, diferem das informações de natureza interna à medida que sua extensão em uma eventual divulgação, poderia afetar significativamente os negócios da DOURO, seus clientes, sócios e



colaboradores. Exemplos: registros de funcionários, planos salariais, informações sobre clientes, sejam elas genéricas ou específicas.

Sua divulgação é proibida, salvo se solicitada por órgão fiscalizador competente (BACEN, CVM e Receita Federal, por exemplo), situação na qual deverá ser prestada por uma das seguintes pessoas: Contador, Controller, Auditor Interno, Advogado ou um dos sócios.

**INFORMAÇÕES ALTAMENTE RESTRITAS:** Correspondem a mais alta classificação de segurança para as informações que transitam na DOURO. Destina-se às informações cuja divulgação não autorizada, provavelmente provocaria danos substanciais, constrangimentos ou penalidades à DOURO, seus clientes, sócios ou colaboradores. As pessoas designadas para o tratamento e uso de tais informações, têm a responsabilidade de garantir que elas sejam devidamente protegidas e seguramente armazenadas quando não estiverem em uso. Exemplos: informação antecipada e não autorizada de novos produtos ou serviços, informações de fusões, aquisições ou outras atividades do mercado de capitais não disponíveis ao público em geral.

Tal como telefone, fax, carta e outros documentos, o e-mail também é forma de comunicação de uso da DOURO, cujo objetivo é tornar suas atividades mais rápidas e fáceis. O e-mail também caracteriza um compromisso com terceiros, sejam eles clientes ou prestadores de serviço, e equivale aos papéis timbrados da DOURO, portanto, o uso desta ferramenta deve ser feito de formacautelosa, profissional e com linguagem adequada.

Como se trata de ferramenta de trabalho de propriedade da DOURO, ela se reserva ao direito de rastrear, monitorar, gravar e inspecionar quaisquer informações transmitidas através de correspondência eletrônica, sem prévio aviso, com objetivo de evitar riscos decorrentes de ataques externos e do mau uso da ferramenta. Os Colaboradores, com a aceitação dos termos e condições desta Política, autorizam a DOURO a acessar as informações transmitidas e recebidas em suas contas de e-mail, ficando cientes de que o uso indevido ou não autorizado os sujeitará a punições. Todos os emails enviados, principalmente aqueles com arquivos anexados, devem ser rigorosamente checados e enviados com o máximo cuidado com relação ao destinatário para evitar que informações confidenciais ou de uso restrito se extraviem.

Com relação ao uso do e-mail, algumas práticas são proibidas. São elas:

- i) Assediar ou perturbar outrem seja através de linguagem inadequada, alta frequência de mensagens ou excessivo tamanho de arquivos;
- ii) Enviar quantidade excessiva de mensagens de e-mail em lote ("junk mail" ou "spam") ou e-mails mal-intencionados ("mail bombing") que, de acordo com a capacidade técnica da rede, seja prejudicial ou sobrecarregue intencionalmente usuários, site, servidor, etc;



- iii) Reenviar ou, de qualquer forma, propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens; e
- iv) Cadastrar em sites de compras e entretenimentos o e-mail corporativo como contato.

## **6. SENHAS E DIREITO DE ACESSO**

### **6.1. SENHAS**

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso. Cabe aos usuários a memorização de suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário e números sequenciais, etc.

Mecanismos para elaboração de senhas:

- Utilize preferencialmente senhas distintas para usos distintos, evitando repetir senhas de uso pessoal para acessos corporativos.
- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Desta forma, evite o uso de dados pessoais, sequencias de teclado, palavras que fazem parte de listas publicamente conhecidas (times de futebol), por exemplo.
- Selecione caracteres de uma frase: "Eu trabalho na DOURO há 3 anos e 1 mês": EtnHh3a1m
- Utilize uma frase longa, como parte de uma música, por exemplo: "Ninguém segura a juventude do Brasil"
- Faça substituição de caracteres semelhantes: "Astro-rei" por "A5tr0-re1"

### **6.2. ACESSOS A SISTEMAS**

A DOURO utiliza em sua plataforma de softwares sistemas adquiridos de terceiros. Para ter acesso a esses, após a admissão o colaborador recém-contratado deve solicitar ao seu gestor o acesso. A senha utilizada para cadastro será genérica e deverá ser modificada após o primeiro acesso por uma senha de uso pessoal e intransferível.

### **6.3. ACESSO A DIRETÓRIOS**

Todos os colaboradores quando admitidos ou transferidos de área receberão um perfil básico e terão acesso à pasta compartilhada de sua área no Drive File Stream.

Qualquer acesso específico do colaborador que seja necessário para o andamento de suas



atividades deverão ser ao gestor imediato do profissional, que deliberará sobre a aprovação ou não do acesso.

#### 6.4. ACESSO À INTERNET E REDE VIA WI-FI (WIRELESS FIDELITY)

O acesso à Internet é permitido a todos os Colaboradores usuários de computador, com o objetivo de facilitar suas tarefas. Assim como qualquer outro material de trabalho, as páginas da Internet também devem ser usadas somente para fins profissionais. Para uma utilização eficiente e produtiva algumas regras devem ser obedecidas:

- É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, atividades de hacker e quaisquer outras atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento do superior imediato do colaborador.
- Fica proibido o download de arquivos e programas não autorizados.

A intenção desta política é evitar que vírus, cavalos de Tróia e outros programas indevidos, não licenciados e nocivos apareçam no ambiente de computação da DOURO.

O acesso à rede interna via Wi-Fi é permitida para os Sócios, colaboradores e visitantes externos que utilizarão as salas de reunião para apresentações ou auditorias.

#### 6.5. ACESSO AOS AMBIENTES

O acesso de visitantes (inclusive ex-funcionários) no ambiente operacional da DOURO só poderá ocorrer com acompanhamento de funcionário, sendo vedada a circulação de terceiros sem autorização específica para isso.

#### 6.6. PROCEDIMENTOS DE RETIRADA DE ACESSO

Quando um colaborador é desligado da DOURO, ele perde imediatamente o direito de acesso aos diversos ambientes de rede, serviço de e-mail externo e internet. Este procedimento é iniciado quando do envio de Check List de desligamento, quando as áreas responsáveis pelos acessos deverão providenciar o cancelamento das credenciais de acesso de profissional.

Os trabalhos desenvolvidos ou elaborados pelo colaborador pertencem exclusivamente à DOURO, não cabendo ao associado o direito de retirá-lo ou copiá-lo quando de seu desligamento, não sendo permitida a gravação de arquivos em qualquer mídia sem a devida autorização.

## **7. SOFTWARE E COMPUTADORES**

Para mantermos o ambiente lógico, todos os softwares/aplicações operacionais devem ser homologados pelos usuários das áreas envolvidas, que devem verificar os impactos das novas versões nos procedimentos, resultados e impostos.

**Aquisição:** A aquisição de softwares ocorrerá conforme planejamento orçamentário, após validação das necessidades de uso pela diretoria da empresa.

**Distribuição:** Os computadores são disponibilizados conforme necessidades de uso de cada colaborador, com base nos softwares destinados à automação de sua área. As impressoras ficarão distribuídas em centros de impressão, localizados em pontos que melhor atendam a maioria dos colaboradores e não estejam em áreas que impliquem em risco à segurança do patrimônio.

**Propriedade:** Os softwares, incluindo os desenvolvidos internamente, e recursos computacionais diversos pertencem exclusivamente à DOURO, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas e criações intelectuais elaboradas e desenvolvidas pelos Colaboradores, Prestadores de Serviços e Consultores, durante a vigência da relação de emprego ou relação contratual.

### **7.1. VÍRUS**

A qualquer indício de existência de vírus, o colaborador deve interromper suas tarefas e comunicá-lo imediatamente ao superior, que executará os procedimentos para a erradicação de vírus determinados na Política de Segurança. Os esforços individuais e isolados dos usuários para acabar com os vírus podem contribuir para provocar danos ainda maiores, pois, em geral, estes usuários não estão capacitados para esta atividade.

O uso de softwares freeware ou shareware e arquivos em outras mídias constituem formas muito comuns de transferência de vírus para os computadores, portanto, sua utilização sem a prévia autorização da TI Infraestrutura é terminantemente proibida.

### **7.2. HARDWARES E SOFTWARES PESSOAIS**

Equipamentos de utilização pessoais, tais como Blackberry, Notebook ou Aparelho de Telefone Celular, são cedidos aos colaboradores para que desenvolvam suas atividades profissionais, sendo obrigatória a assinatura de um termo assumindo toda a responsabilidade pelos mesmos e pelos softwares neles instalados.



## **8. NOTIFICAÇÃO DE INCIDENTES E ABUSOS**

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas e redes. Alguns exemplos são: tentativa de uso ou acesso não autorizado a sistemas e dados, tentativa de tornar serviços indisponíveis, desrespeito à política de segurança.

É responsabilidade dos colaboradores notificar sempre que se deparar com uma atitude que considere abusiva ou com um incidente de segurança para que sejam tomadas as devidas ações, minimizando os impactos da ocorrência.