D'GOLD

Manual de Controles Internos Políticas e Normas

DA POLÍTICA DE SEGURANÇA CIBERNÉTICA
ASPECTOS GERAIS

0. INTRODUÇÃO

O objetivo do presente documento é atender a Resolução nº 4.658/2018 do Banco Central do Brasil e determinar as práticas a serem adotadas por todos os administradores, funcionários, estagiários e prestadores de serviços regulares da D'Gold. A informação é um dos principais bens de qualquer empresa, e a D´GOLD estabelece a presente Política de Segurança Cibernética a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da D´GOLD e de seus clientes em geral, as quais devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida. Esta Política está organizada de forma a dar pleno entendimento às determinações da referida Resolução, de acordo com os tópicos nomeados a seguir:

1. Visão Geral

2. Política de Segurança Cibernética
3. Prevenção do Vazamento de Informações
4. Gestão de Riscos;
5. Detecção de Intrusão
6. Proteção Contra Software Malicioso
7. Mecanismos de Rastreabilidade 8. Estratégia de Contingência
9. Regras para Contratação de Serviços na Nuvem
10. Gestão de Mudanças

1. VISÃO GERAL

O objetivo deste documento é determinar os objetivos, procedimentos e controles da D'Gold que atendam aos requisitos da Resolução 4.568 de 26/04/2018. O seu escopo refere-se à toda e qualquer informação acessada ou utilizada pelos administradores, funcionários, estagiários ou prestadores de serviços regulares, bem como os recursos computacionais e de sistemas utilizados internamente ou na nuvem (cloud computing). O conteúdo desde documento está totalmente aderente à missão e aos valores corporativos da D'GOLD e está baseado em normas ISO consolidadas e nas boas práticas de mercado.

1.1. OBJETIVO DA SEGURANÇA CIBERNÉTICA

A segurança cibernética tem como objetivo básico minimizar a vulnerabilidade da D'GOLD a incidentes de qualquer ordem, de modo a preservar suas informações confidenciais e garantir a continuidade de seus negócios. Na abordagem da Resolução 4.658, a segurança cibernética está direcionada à contratação e execução de serviços na nuvem e devem prover: a. Rastreabilidade das informações sensíveis, com níveis de necessidade e confidencialidade determinados pelo responsável pela gestão; b. Registro, análise de impacto e o controle dos efeitos de eventuais incidentes;

1.2. GESTÃO DE RISCO

A segurança cibernética da D'GOLD contempla as seguintes ferramentas para a gestão de risco:
a. Compliance;
b. Classificação de Informações;
c. Análise de Impacto;
d. Plano de Contingências;

e. Plano de Teste de Continuidade de Negócios;

1.3. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

Para que a cultura de segurança cibernética seja disseminada e efetiva, estão à disposição de todos os administradores, funcionários, estagiários e prestadores de serviços regulares da D'GOLD os seguintes mecanismos: a. Divulgação na Intranet; b. Treinamento e avaliação periódica; c. Divulgação junto aos clientes e usuários sobre as precauções no uso de produtos e serviços financeiros; d. Compromisso com alto nível de maturidade e com a melhoria contínua;

1.4. FUNDAMENTOS DA SEGURANÇA CIBERNÉTICA

É obrigação da D'GOLD proteger suas informações, sejam estas as contidas em base eletrônica de dados, impressas, manuscritas ou mesmo verbais. As ferramentas que suportam esta proteção deverão estar baseadas em:

a. Controle de Acesso:
i. Do acesso ao local de trabalho;
ii. Do acesso às dependências com valores monetários;
iii. Do controle de acesso a sistemas de informação;

b. Análise de Risco:
i. Plano de Contingências;
ii. Normas de contratação de serviços;

Estes fundamentos estão baseados nas recomendações da Norma ISO 27002

2. POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Política de Segurança Cibernética possui na sua formação o agrupamento das regras formais para o tratamento das informações por todos os administradores, funcionários, estagiários e prestadores de serviços regulares da D'GOLD, de modo a prover a devida proteção no uso e compartilhamento de informações. As atribuições de responsabilidade no tratamento destas informações deverão estar demonstradas por uma Matriz de Responsabilidades.

2.1. DEFINIÇÃO BÁSICA DE INFORMAÇÃO

Informação é um dado ou conteúdo que possua valor para o negócio, não importando que esteja armazenada num banco de dados corporativo, num dispositivo qualquer, numa folha de papel (impressa ou manuscrita) ou ainda de caráter verbal. Portanto, em todas as suas formas, a importação deverá ser classificada e protegida.

Esta proteção é uma obrigação individual de quem teve acesso à mesma e pressupõe a devida cautela em:
a. Manter acessos a sistemas e documentos protegidos por senhas não usuais;
b. Imprimir relatórios;
c. Anotar informações de forma manuscrita;
d. Descartar informações na lata de lixo;

e. Circular informações verbalmente, dentro e fora do ambiente da empresa;

2.2. CARACTERÍSTICAS BÁSICAS DA SEGURANÇA CIBERNÉTICA

A segurança cibernética possui um conjunto de características básicas, que determinam o padrão de certificação da segurança, para que se reduzam os riscos com incidentes de divulgação indevida, fraudes, erros propositais ou não, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer essas características básicas.

2.2.1. CONFIDENCIALIDADE

Proteção da informação compartilhada contra acessos não autorizados. A ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostos voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um conjunto determinado de usuários.

2.2.2. INTEGRIDADE

Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. A ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

2.2.3. DISPONIBILIDADE

Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. A ameaça à segurança acontece quando a informação deixa de estar acessível para quem necessita dela.

2.2.4. CONTROLE DE ACESSO

O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso.

A ameaça à segurança acontece há descuido, falha ou possível quebra da confidencialidade das senhas de acesso à rede.

3. PREVENÇÃO DO VAZAMENTO DE INFORMAÇÕES

Trata-se de um conjunto de ações e responsabilidades voltadas a prevenir o vazamento indevido de informações, de qualquer forma ou natureza, em poder da D'GOLD.

3.1. REGRAS DE USO DA TECNOLOGIA

A tecnologia disponibilizada pela D'GOLD é autorizada exclusivamente para o usuário desempenhar suas atribuições na empresa, de acordo com os termos de uso e autorizações concedidos e aceitos.

3.1.1. COMUNICAÇÃO

Quando o usuário se comunicar através de recursos de tecnologia da D'GOLD, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da empresa.

3.1.2. CONTEÚDO

Os conteúdos acessados e transmitidos através dos recursos de tecnologia da D'GOLD devem ser legais, de acordo com o Código de Ética e Conduta, e devem contribuir para as atividades profissionais do usuário.

3.1.3. AUDITORIA INTERNA

O uso dos recursos de tecnologia da D'GOLD poderá ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente.

3.1.4. RESPONSABILIDADE

Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados.

3.1.5. CONFIDENCIALIDADE

Os recursos de tecnologia da D'GOLD, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização. Ao identificar qualquer irregularidade nos recursos de tecnologia disponibilizados pela D´GOLD, o usuário deve comunicar imediatamente ao gestor da Política de Segurança Cibernética.

3.2. REGRAS DE USO DO RECURSO COMPUTACIONAL

Aqui serão definidas as regras para uso de qualquer recurso computacional da D'GOLD disponibilizados a seus usuários.

3.2.1. PROPRIEDADE DO RECURSO COMPUTACIONAL

O recurso computacional disponibilizado para o usuário exercer suas funções profissionais na empresa é de propriedade da D'GOLD.

3.2.2. DISPONIBILIZAÇÃO E USO

O recurso computacional disponibilizado para o usuário pela D'GOLD tem por objetivo o desempenho das atividades profissionais desse usuário dentro da organização.

3.2.3. AUTORIZAÇÃO PARA USO

É necessário que o gestor do usuário o autorize a usar o computador ou qualquer outro recurso computacional. Deverá ser feita uma solicitação à área de infraestrutura da Tecnologia (TI), que autorizará tecnicamente e fará a liberação mediante a disponibilidade de recursos. A D'GOLD poderá a qualquer momento retirar ou substituir o computador ou qualquer outro recurso computacional disponibilizado

para qualquer usuário.

3.2.4. QUALIDADE DO RECURSO COMPUTACIONAL

Todos os equipamentos, softwares e permissões de acessos deverão ser testados, homologados e autorizados pela área de infraestrutura da Tecnologia (TI) para uso na exclusivo na D'GOLD

3.2.5. RESPONSABILIDADE

Cada recurso computacional possui o seu gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área de infraestrutura da Tecnologia (TI).

3.2.6. ACESSO AO RECURSO COMPUTACIONAL

a. A identificação do usuário ao computador é feita através do login e senha disponibilizado pela área de Infraestrutura da Tecnologia (TI), portanto ela é sua assinatura eletrônica, pessoal e intransferível;

b. Será permitido apenas definições de senhas fortes com no mínimo 8 caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 5 vezes;

c. É permitido apenas 3 tentativas máximas de autenticação de senha, sendo que na ocorrência de 3 tentativas malsucedidas, o acesso será automaticamente bloqueado;

d. A senha possui validade de 180 dias e sua troca será solicitada automaticamente quando do fim do prazo de validade;

3.2.7. USABILIDADE DE PROGRAMAS E APLICATIVOS

a. Os sistemas e programas básicos (sistema operacional e ferramentas) e componentes físicos serão implantados e configurados pela área de infraestrutura da Tecnologia (TI);

b. É vedado aos usuários implantar novos programas e sistemas, ou alterar configurações sem a permissão formalizada da área de infraestrutura da Tecnologia (TI);

c. É vedado aos usuários implantar ou alterar componentes físicos no computador ou em qualquer outro recurso computacional;

3.2.8. HISTÓRICO DE VERIFICAÇÃO DO COMPUTADOR E DOS ACESSOS

A D'GOLD manterá por 5 anos todos os logs e registros de acesso aos sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados pelas áreas de infraestrutura da Tecnologia (TI) e Compliance.

Os acessos a equipamentos, softwares e respectivas permissões serão testados pela área de Infraestrutura da Tecnologia (TI) com validação da área de Riscos e Controles Internos a cada 6 meses.

3.2.9. RESPONSABILIDADES DO USUÁRIO

a. Cuidar adequadamente do equipamento. O usuário é o custodiante deste recurso;

b. Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de infraestrutura da Tecnologia (TI);

3.2.10.OUTRAS PROTEÇÕES

a. Será implementada o mecanismo de proteção de tela nos computadores e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente);

b. Será implantado o "log-off" automático do usuário por inatividade durante o período superior a 24 horas;

c. Será implantado o bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores;

d. Será implantado o bloqueio do acesso à sites de armazenamento de dados em nuvem (cloud); e. Será implantado o bloqueio de sistemas de gerenciamento de computador a distância;

3.2.11.TERMO DE COMPROMISSO

Para ter acesso às informações da D'GOLD, o usuário deverá assinar (manual ou eletronicamente) um termo de compromisso. Os casos de exceção serão definidos pelo Comitê Gestor. (ISO A.8.1.3) O departamento de Compliance da D'GOLD alertará a todos os usuários que a instalação ou utilização de software não autorizados constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/1998, sujeitando os infratores à pena de detenção e multa

A D'GOLD não se responsabilizará por qualquer ação individual que esteja em desacordo com a lei mencionada acima. Todas as práticas que representam ameaças à segurança da informação serão tratadas com a aplicação de ações disciplinares e/ou administrativas.

3.3. REGRAS DE USO DA INTERNET

3.3.1. RESPONSABILIDADE E FORMA DE USO

a. O usuário é responsável por todo acesso realizado com a sua autenticação;

b. O usuário é proibido de acessar endereços de internet (sites) que:
• Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes;
• Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia;
• Possuam conteúdo político ou vinculado à partidos ou organizações políticas de qualquer ideologia;
• Contenham informações que não colaborem para o alcance dos objetivos da FD'GOLD DTVM;
• Defendam atividades ilegais. Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física;
• Coloquem em risco à reputação e a imagem da D´GOLD;

c. O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de

uso e patentes existentes e que o uso do material foi autorizado pelo gestor da sua área.

d. É proibido o uso de serviços de mensagens instantânea (MSN, SKYPE, WhatsApp, etc.), através dos computadores da F'GOLD, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pelo departamento de Compliance.

e. É proibido o uso de serviços de rádio, TV, download de vídeos, filmes e músicas, através dos computadores da D'GOLD, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pela área de infraestrutura da Tecnologia (TI).

f. Periodicamente a área de infraestrutura da Tecnologia (TI) revisará e bloqueará o acesso aos endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética e Conduta da D´GOLD. g. É proibido o acesso aos serviços de correio eletrônico particular, tipo Webmail, através dos computadores e demais recursos de tecnologia da D'GOLD.

3.4. REGRAS DE USO DO CORREIO ELETRÔNICO CORPORATIVO (E-MAIL)

3.4.1. ENDEREÇO ELETRÔNICO DO USUÁRIO

A D'GOLD disponibilizará endereços de seu correio eletrônico corporativo para utilização dos usuários no desempenho de suas funções profissionais. (ex.: usuario@fdgolddtvm.com.br ou usuario@dgold.-com.br) O endereço de correio eletrônico corporativo disponibilizado para o usuário é individual, intransferível, pertence à D´GOLD e deverá ser o mesmo durante todo o seu período de vínculo com a D'GOLD. Se houver necessidade de troca de endereço de correio eletrônico corporativo, a alteração deverá ser autorizada pela área de infraestrutura da Tecnologia (TI) e registrada para possibilitar uma posterior verificação de histórico e autoria.

3.4.2. CRIAÇÃO, MANUTENÇÃO E EXCLUSÃO DE ENDEREÇO DE CORREIO ELETRÔNICO CORPORATIVO

A utilização desse endereço de correio eletrônico corporativo pelo usuário necessita de autorização pelo Gestor da área. A liberação do endereço de correio eletrônico corporativo será feita somente pela área de infraestrutura da Tecnologia (TI), de maneira controlada e segura, com o objetivo de garantir que apenas o usuário tenha possibilidade de utilizar o referido endereço. Quando acontecer desligamento de usuário, o Gestor deve comunicar à área de infraestrutura da Tecnologia (TI) o nome e a identificação do usuário desligado, para que seja cancelado o acesso ao endereço de correio eletrônico corporativo.

As caixas postais de contas de correio eletrônico corporativo da D'GOLD terão um limite máximo de armazenagem de dados de 3.2GB e as mensagens enviadas/recebidas poderão conter arquivos anexos com até 8MB por mensagem.

3.4.3. ENDEREÇO ELETRÔNICO DE PROGRAMAS OU DE COMUNICAÇÃO CORPORATIVA

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da área de infraestrutura da Tecnologia (TI) responsável por acompanhar as mensagens emitidas e recebidas por esse endereço de correio eletrônico. É permitido a existência de endereços de correio eletrônico para o envio de mensa-

gens tipo Comunicação Interna da D'GOLD, porém, é obrigatória a identificação do usuário que encaminhar as mensagens.

3.4.4. ACESSO À DISTÂNCIA OU REMOTO

O usuário pode acessar o seu endereço de correio eletrônico corporativo cedido pela D'GOLD mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet (Web Mail).

3.4.5. PROPRIEDADES DO ENDEREÇO DE CORREIO ELETRÔNICO

O endereço de correio eletrônico corporativo disponibilizado para o usuário e as mensagens associadas a esse endereço de correio eletrônico, são de propriedade exclusiva da D'GOLD. Em situações autorizadas pela Diretoria, as mensagens do correio eletrônico corporativo de um usuário poderão ser acessadas pela D'GOLD ou por outro usuário, ou ainda por pessoas ou entidades por ela indicadas, inclusive empresas de auditoria interna. Não devem existir expectativa de direito de privacidade pessoal no uso dos endereços de correio eletrônicos corporativos.

3.4.6. RESPONSABILIDADES E FORMA DE USO DE CORREIO ELETRÔNICO

O usuário que utiliza um endereço de correio eletrônico corporativo:

a. É responsável por todo acesso, conteúdo de mensagens e uso relativos a este endereço de correio eletrônico corporativo; b. Poderá somente enviar mensagens necessárias para o desempenho de suas atividades profissionais na D´GOLD; c. É proibido criar, copiar ou encaminhar mensagens ou imagens que: • Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza; • Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais; • Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não; • Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física; • Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional.; • Possuam informações de caráter político; • Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros; • Defendam ou possibilitem a realização de atividades ilegais; • Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
• Possam prejudicar a imagem da D'GOLD;
• Sejam incoerentes com o Código de Ética e Conduta;

d. É proibido reproduzir qualquer material recebido pelo correio eletrônico corporativo ou por qualquer outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da D´GOLD.

e. Deverá estar ciente de que uma mensagem de correio eletrônico corporativo da D'GOLD é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da D´GOLD.

f. É proibido de emitir qualquer opinião pessoal, colocando-a em nome da D'GOLD, exceto quando especificamente autorizado para tal.

g. Deverá observar se o endereço de correio eletrônico do destinatário corresponde realmente ao des-

tinatário da mensagem desejado.

h. Deverá ser diligente em relação:

• Aos usuários que receberão as mensagens (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
• Ao nível de sigilo das informações contidas nas mensagens enviadas;
• Aos anexos das mensagens enviadas, enviando arquivos apenas quando for imprescindível e garantindo a sua confidencialidade;
• Ao uso da opção "Encaminhar" (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas;
• A inclusão de mensagem de ausência quando for passar um período maior do que 48 horas sem acessar seu correio eletrônico corporativo, que deverá indicar o período de ausência e o endereço de correio eletrônico corporativo de seu substituto para quem deverão ser encaminhas as mensagens durante a sua ausência;

3.4.7. CÓPIAS DE SEGURANÇA

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria: A cópia de segurança das mensagens de correio eletrônico corporativo será feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área de infraestrutura da Tecnologia (TI).
A área de infraestrutura da Tecnologia (TI) fornecerá o serviço de recuperação de mensagens de correio eletrônico corporativo, a partir de arquivos de cópia de segurança, cumprindo parâmetros de nível de serviço previamente estabelecidos.

3.5. REGRAS DE USO DO TELEFONE 3.5.1.

NÚMERO DO TELEFONE DO USUÁRIO A D'GOLD disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais. Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela área de infraestrutura da Tecnologia (TI) e registrada para possibilitar uma posterior verificação de autoria.

3.5.2. PROPRIEDADE DO NÚMERO DO TELEFONE

O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade exclusiva da D'GOLD. Todas as ligações telefônicas serão gravadas e monitoradas regularmente, e em situações especiais autorizadas pelo Comitê Gestor, as conversas de um usuário poderão ser acessadas pela D'GOLD ou por pessoas/entidades por ela indicada, inclusive empresa de auditoria. Desta forma, não deverá ser mantida expectativa de privacidade pessoal com relação as ligações telefônicas.

3.5.3. RESPONSABILIDADES E FORMA DE USO

O usuário que utiliza um telefone:
• É responsável por todo conteúdo da conversa.;
• Deverá utilizar o telefone apenas para o desempenho de suas atividades profissionais na D´GOLD.
• É proibido utilizar o telefone para conversas que:
• Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza.

• Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física.
• Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional.
• Possuam informação de caráter político de qualquer ideologia.
• Defendam ou possibilitem a realização de atividades ilegais.
• Possam prejudicar a imagem da D'GOLD.
• Sejam incoerentes com o Código de Ética e Conduta da D´GOLD. 3.5.4. CÓPIAS DE SEGURANÇA Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:
• A cópia de segurança das ligações telefônicas será feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área de infraestrutura da Tecnologia (TI).
• A área de infraestrutura da Tecnologia (TI) apenas fornecerá a recuperação de cópia de segurança das ligações telefônicas, a partir de arquivos de cópia de segurança, em situações autorizadas pelo Comitê Gestor.

3.6. CLASSIFICAÇÃO DE INFORMAÇÕES SENSÍVEIS

Consiste no nível de acesso às informações geradas pelos sistemas da D'Gold internamente ou de qualquer forma geradas ou recebidas pela D´GOLD. A classificação passa a ser definida como:

a) Restrito – Documento com acesso somente aos administradores da D'Gold;

b) Público – Documento com acesso livre;

c) Secreto – Documento com acesso somente para a Diretoria da D´GOLD. As informações de uso restrito ou secreto somente poderão ser geradas por usuários com direito de uso restrito ou secreto, dependendo do caso. As informações de uso público poderão ser geradas por qualquer usuário da D'Gold devidamente identificado.

As informações poderão constar da Intranet D'Gold, desde que tenham o nível de divulgação devidamente classificado. Deverá existir um índice indicando as informações existentes e as suas respectivas classificações de sigilo.

4. GESTÃO DE RISCOS

Consiste na previsão, análise de impacto e ações de mitigação dos riscos. A gestão está baseada num Plano de Riscos, que considera as seguintes informações:

4.1. IDENTIFICAÇÃO DO RISCO

Informações de identificação do risco.

4.1.1. ID Identificador do item de risco.

4.1.2. DATA DA IDENTIFICAÇÃO

Data da identificação do risco.

4.1.3. RISCO

Denominação do risco;

4.1.4. CATEGORIA

Categoria do risco. Pode ter os seguintes valores:
• Custo
• Escopo
• Prazo
• Qualidade

4.1.5. PROBABILIDADE

Probabilidade de que o risco aconteça. Pode ter os seguintes valores:
• Alta
• Média
• Baixa

4.1.6. IMPACTO PREVISTO

Tipo de impacto possível. Pode ter os seguintes valores:
• Alto
• Médio
• Baixo

4.1.7. CONSEQUÊNCIAS

Descrição das consequências previstas caso o risco aconteça.

4.1.8. EXPOSIÇÃO

Descrição do produto do impacto caso o risco aconteça.

4.1.9. INDICADOR

Utilizado para monitorar a evolução e/ou ocorrência do evento associado ao risco.

4.1.10.VALOR DE REFERÊNCIA

Valor de referência para análise do indicador.

4.2. RESPOSTA AO RISCO

Informações referentes às ações de controle e/ou mitigação do risco.

4.2.1. RESPONSÁVEL

Nome do responsável pelo controle e/ou mitigação do risco.

4.2.2. AÇÃO

Descrição das ações que possibilitem o controle e/ou a mitigação do risco. As ações de contingência para as situações mais críticas devem ser explicitadas.

4.2.3. ESTRATÉGIA PARA A AÇÃO

Descrição da estratégia a ser adotada para que a ação seja executada.

4.2.4. DATA PARA A AÇÃO

Data prevista para a execução da ação.

4.2.5. CLASSIFICAÇÃO DO RISCO

Descrição dos fatores de risco e as áreas afetadas. (Por exemplo: Tempo/Compliance)

4.2.6. IMPACTO

Tipo de impacto após a ação. Pode ter os seguintes valores:
• Alto
• Médio
• Baixo

4.2.7. SITUAÇÃO

Descrição da situação após a ação.

5. DETECÇÃO DE INTRUSÃO

A detecção de intrusão é realizada através de um software IPS (Intrusion Prevention System). O IPS deverá ser capaz de:
• Enviar um alarme ao administrador;
• Derrubar pacotes maliciosos;
• Bloquear o tráfego a partir do endereço de origem;
• Redefinir a conexão;

Como deverá estar o tempo todo on-line, o IPS deve trabalhar eficientemente, não influindo significativamente no desempenho de rede, além de manter alta velocidade na identificação dos eventos, sabendo-se que muitos deles podem ocorrer em tempo real. Uma outra característica é a alta precisão na detecção de ameaças, de modo a eliminá-las e aos falsos positivos.

5.1. METODOLOGIA DA DETECÇÃO DE INTRUSÃO

O IPS deve abrange vários métodos de detecção. Entretanto, os mecanismos mais usados por invasores são:
• Assinatura
• Anomalias estatísticas

5.1.1. ASSINATURA

A detecção baseada em assinatura possuirá como referência um dicionário de padrões de assinaturas que podem ser identificadas no código de cada "exploit". Quando esse "exploit" é descoberto, sua assinatura é armazenada em um dicionário de referência de assinaturas. A detecção de assinaturas de "exploits" para o IPS se divide em dois tipos:

• Assinaturas encarregadas de reconhecer "exploits" individuais no fluxo de tráfego;
• Assinaturas encarregadas de reconhecer "exploits" que exploram as vulnerabilidades do ambiente.

Essas assinaturas protegem contra variações de um "exploit" que podem ainda não ter sido diretamente detectado;
Entretanto, nesse caso, é possível a detecção de falsos positivos.

5.1.2. ANOMALIAS ESTATÍSTICAS

A detecção de anomalias estatísticas é baseada em estudo de uma amostragem do tráfego de rede, para comparar com um padrão determinado. Quando a amostragem identifica um desvio do padrão determinado, o IPS age na solução da ameaça identificada.

6. PROTEÇÃO CONTRA SOFTWARE MALICIOSO

Os computadores da rede e os servidores na nuvem deverão estar protegidos por um software de firewall e antivirus, de mercado com qualidade comprovada.

Além dessa medida, outras medidas devem ser orientadas para ajudar a prevenir a entrada de software malicioso, tais como:
• Programar as regras de recebimento de e-mails para detectar spam, black list e e-mails suspeitos;
• Caso o e-mail seja suspeito e tenha passado pelas regras, o usuário não deve clicar em links ou botões no corpo do e-mail, e deve notificar a área de infraestrutura da Tecnologia (TI) sobre a ocorrência;
• Não entrar em páginas de internet classificadas pelo antivírus como suspeitas, notificando a área de infraestrutura da Tecnologia (TI);

7. MECANISMOS DE RASTREABILIDADE

Para garantir a rastreabilidade dos processos executados pela D'Gold, os seguintes instrumentos são utilizados:

7.1. SISTEMAS DE INFORMAÇÃO

Serão gerados os registros cronológicos (logs) de acesso e uso dos sistemas, baseados no acesso de cada usuário válido.

Estes logs poderão ser consultados a qualquer momento pelos usuários com
essa autoridade.

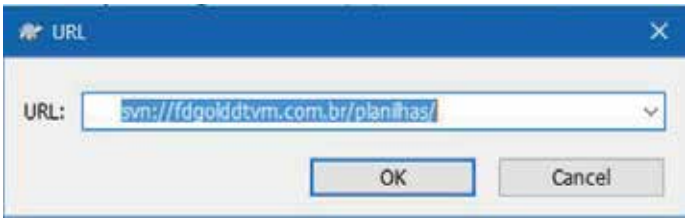
Abaixo, um exemplo do log.

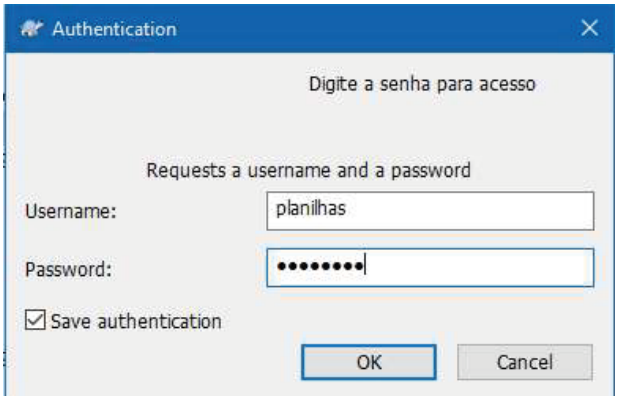
7.2. ARQUIVOS DE APOIO (PLANILHAS, DOCUMENTOS E APRESENTAÇÕES)

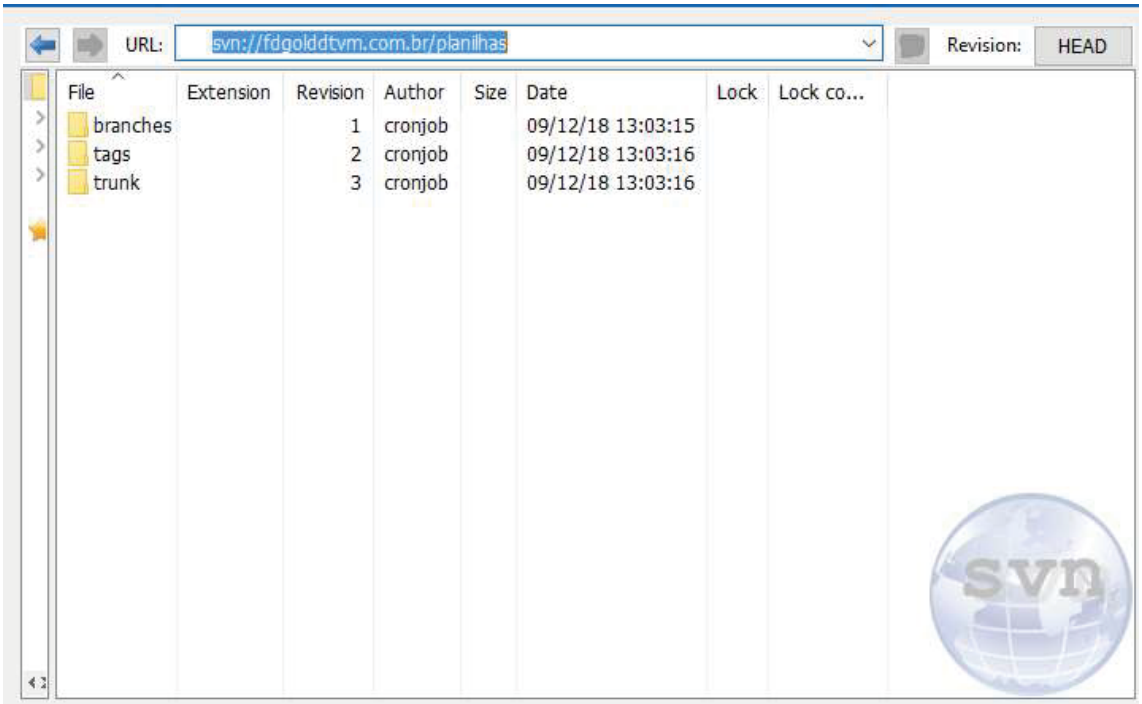
Os arquivos de apoio possuem repositório no servidor na nuvem, tendo suas versões controladas por um controle de repositório (SVN – Apache Subversion).

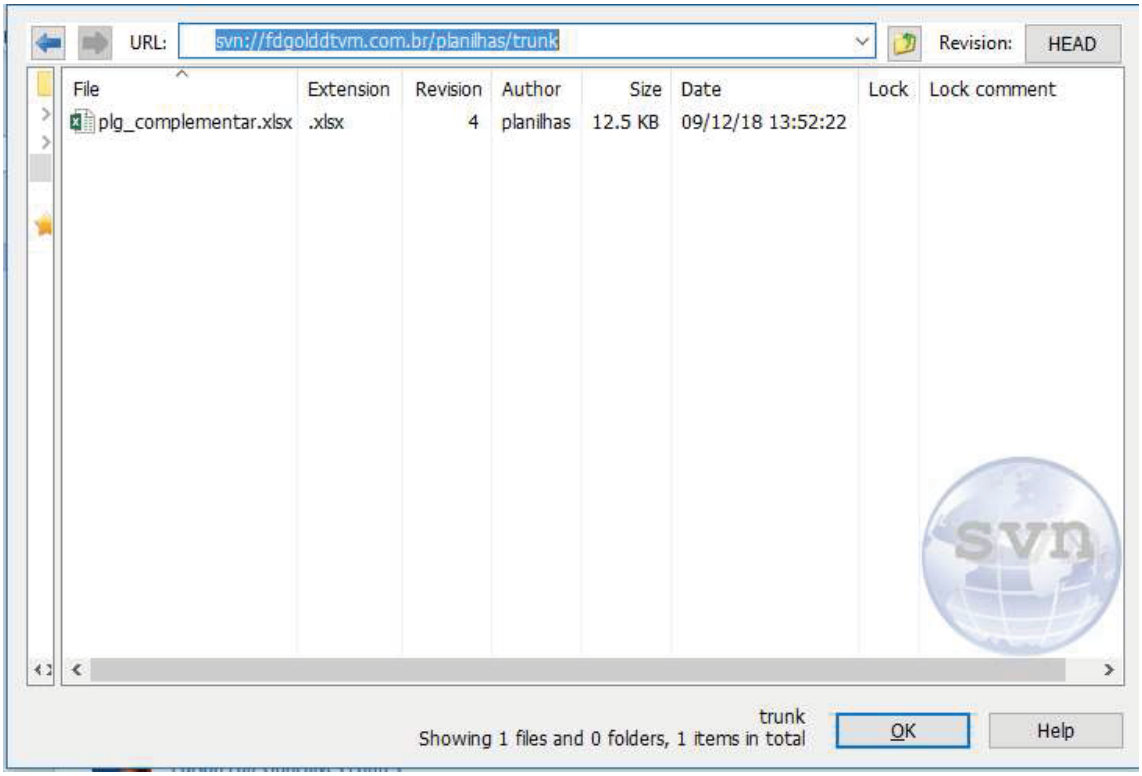
Cada usuário terá uma conta no SVN e deverá usá-la para baixar a última versão ou a versão desejada para a sua estação de trabalho.

Abaixo, um exemplo do uso do SVN.






URL:
svn://fdgolddtvm.com.br/planilhas
Revision:
HEAD
File
Extension
Revision
Author
Size
Date
Lock
Lock co...
branches
1
cronjob
09/12/18 13:03:15
tags
2
cronjob
09/12/18 13:03:16
trunk
3
cronjob
09/12/18 13:03:16
SVN


URL:
svn://fdgolddtvm.com.br/planilhas/trunk
Revision:
HEAD
File
Extension
Revision
Author
Size
Date
Lock
Lock comment
plg_complementar.xlsx
.xlsx
4
planilhas
12.5 KB
09/12/18 13:52:22
SVN
trunk
Showing 1 files and 0 folders, 1 items in total
OK
Help

8. ESTRATÉGIA DE CONTINGÊNCIA

A estratégia de contingência para o ambiente cibernético deverá conter:

8.1. MEDIDAS DE PREVENÇÃO

a) Estabelecimento de plano de contingência, prevendo as ações de retomada, no caso de incidente motivador de paralisação do acesso aos sistemas ou documentos, plano de comunicação e SLA (Service Level Agreement);

b) O plano de contingência deve prever ações no caso de incidentes na sede da D'Gold ou nas empresas contratadas para armazenamento e processamento na nuvem, onde estarão os servidores principal e de contingência;

c) Para o caso de incidente na sede da D'Gold, o plano de contingência deverá prever o novo local onde o negócio deverá ter continuidade;

d) Um incidente na D'Gold não alterará o funcionamento dos postos de compra de ouro bruto, em virtude de os servidores encontrarem-se na nuvem;

e) Para o caso de incidente no servidor principal, será acionado o servidor de contingência, e a liberação será comandada pela equipe de contingência da D'Gold;

f) Configuração de servidor de contingência, espelhando o estado do servidor principal, de forma a garantir a continuidade do negócio;

g) Os dados armazenados no servidor principal deverão ser replicados em tempo real no servidor de contingência, de forma a garantir imediata recuperação da atividade empresarial;

h) Verificação periódica da disponibilidade e integridade de dados do servidor principal e do servidor de contingência;

i) Treinamento periódico dos colaboradores envolvidos com o plano de contingência;

j) Plano de testes de continuidade de negócios;

k) Registro devidamente documentado dos testes de continuidade de negócios com frequência no mínimo semestral;

8.2. MEDIDAS DE AÇÃO

a) Identificar o incidente;

b) Caso o incidente seja na sede da D'Gold:
• Não afeta diretamente os postos de compra de ouro bruto;
• Os colaboradores da equipe de contingência deverão dirigir-se ao local determinado para processamento da contingência e dar prosseguimento ao trabalho;
• Ao ser restabelecida a normalidade na sede da D'Gold, os colaboradores da equipe de contingência deverão voltar à sede para continuidade das atividades;

c) Caso o incidente seja no servidor principal, a equipe de contingência deverá:
• Comunicar aos usuários a paralisação momentânea dos serviços, informando um prazo para retomada, de acordo com o SLA (Service Level Agreement) estabelecido no plano de contingência;
• Verificar a integridade dos dados no servidor de contingência;
• Mudar a rota dos sistemas para o endereço IP do servidor de contingência, inclusive para o DNS (Domain Name System);
• Testar o acesso dos usuários aos sistemas;
• Liberar a continuidade dos serviços.

9. REGRAS PARA CONTRATAÇÃO DE SERVIÇOS NA NUVEM

A contratação de serviços na nuvem deverá contemplar as seguintes regras:

9.1. JUSTIFICATIVAS PARA CONTRATAÇÃO DE SERVIÇOS NA NUVEM

A administração da D´GOLD, a partir de justificativas técnicas da área de infraestrutura da Tecnologia (TI), deverá concordar com um termo de contratação de serviços na nuvem de empresas no Brasil ou no Exterior.

9.2. PARÂMETROS PARA CONTRATAÇÃO

Para que os serviços na nuvem sejam contratados, a D'Gold estabelecerá os seguintes parâmetros para a potencial prestadora de serviços:

a) Comprovação de capacidade técnica levando em conta, inclusive, o potencial de crescimento da demanda;

b) Comprovação de idoneidade e de cumprimento da legislação e da regulamentação vigentes;

c) Que a D'Gold tenha acesso garantido aos dados processados e/ou armazenados na empresa contratada;

d) Garantia de confidencialidade, integridade, disponibilidade e recuperação dos dados processados e/ou armazenados na empresa contratada;

e) Comprovação das certificações técnicas estabelecidas pela D'Gold;

f) Acesso da D'Gold aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

g) Acesso às informações de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

h) Garantia da segregação dos dados dos clientes da D'Gold;

i) Garantia de qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da D'Gold;
j) No caso da execução de aplicativos por meio da internet, a D'Gold deverá assegurar que o prestador

b) A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes da D´GOLD;

c) A obrigatoriedade, em caso de extinção do contrato, de:
• transferência dos dados armazenados, processados ou gerenciados ao novo prestador de serviços ou à D'Gold;
• exclusão dos dados pela empresa contratada substituída, após a transferência e a confirmação da integridade e da disponibilidade dos dados recebidos pela nova empresa;

d) Acesso da D'Gold às informações prestadas na proposta de contratação, relativamente aos itens a e b.

e) Informações comprovadas de certificações e relatórios de auditoria da prestadora de serviços;

f) Informações comprovadas sobre os recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) A obrigação de notificação à D'Gold sobre a subcontratação de serviços relevantes relacionados ao objeto do contrato de prestação de serviços;

h) A permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

i) A adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil;

j) A obrigação da prestadora de serviço em manter a D'Gold permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

k) O contrato mencionado no caput deve prever, para o caso da decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

• a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada;

• A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

* a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

* a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada

dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo; A D'Gold deverá possuir recursos e competências necessárias para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso de recursos.

9.3. RESPONSABILIDADES DA FD'GOLD DTVM

Na contratação dos serviços na nuvem são responsabilidades da D'Gold:

a) Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação vigentes.

b) A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada pela D'Gold ao Banco Central do Brasil, com antecedência mínima de 60 (sessenta) dias, informando:

• Nome da empresa contratada;

• Tipo dos serviços contratados;

• Países e regiões de cada país, no caso de contratação no exterior Eventuais alterações contratuais também deverão ser comunicadas ao Banco Central do Brasil com antecedência mínima 60 (sessenta).

c) No caso de contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem no exterior, os seguintes requisitos devem ser atendidos e comprovados:

• A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados. Caso não exista esse convênio, a prestadora de serviço somente poderá ser contratada com autorização do Banco Central do Brasil;

• A D'Gold deverá assegurar que a prestação dos serviços a serem contratados não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

• A D'Gold deverá assegurar que a legislação dos países onde os serviços serão prestados não restrinjam ou impeçam o acesso do Banco Central do Brasil às suas informações;

• Planejamento prévio dos países e das regiões em cada país onde haverá processamento, gerenciamento ou armazenamento de dados;

• A D'Gold deverá prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação destes serviços;

9.4. ITENS DOS CONTRATOS DE PRESTAÇÃO DE SERVIÇOS NA NUVEM

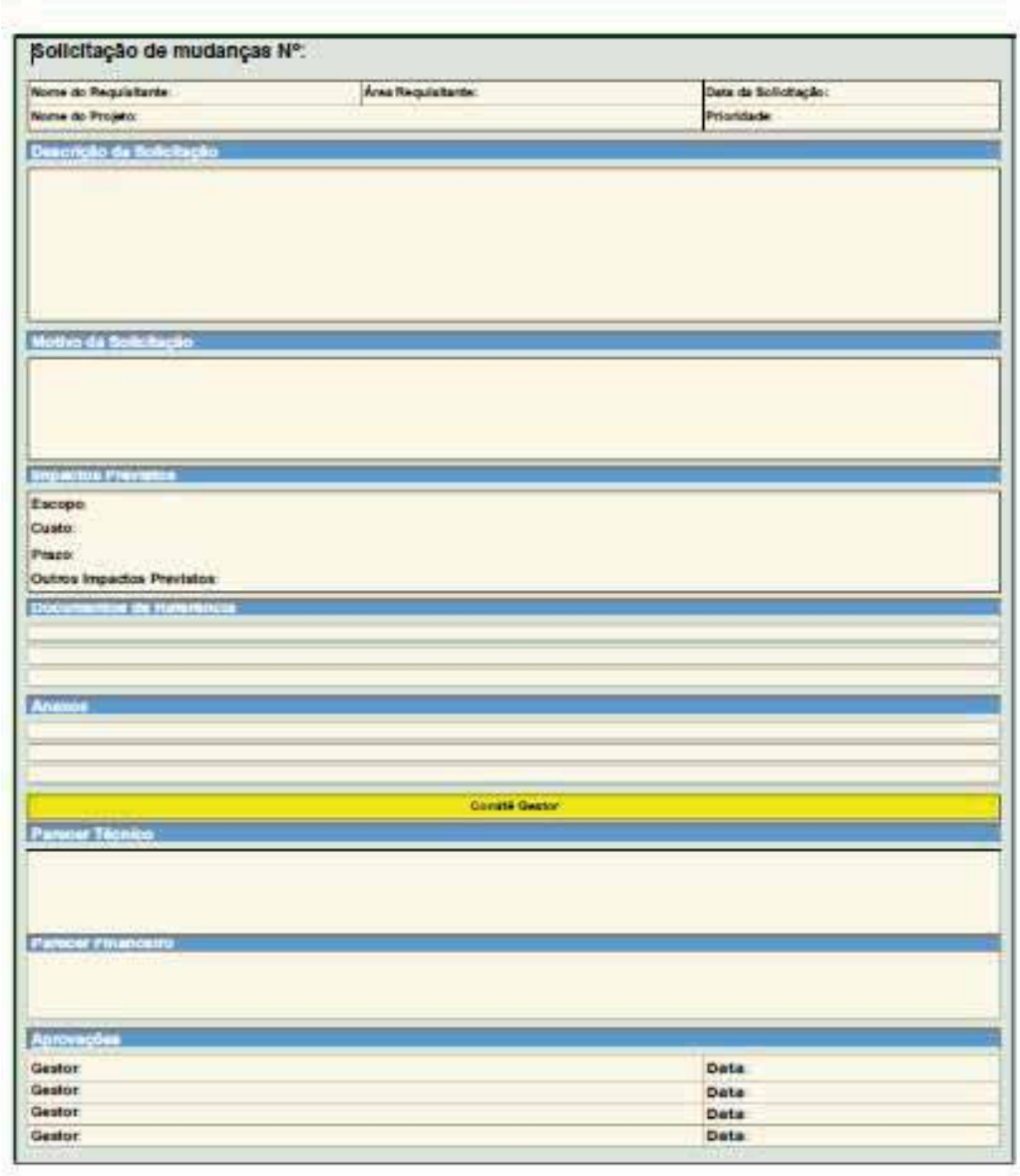
Na contratação dos serviços na nuvem devem constar os seguintes itens:

a) A indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados que poderão ser armazenados, processados e gerenciados, com a comprovação da adoção de medidas de segurança para a transmissão e armazenamento dos dados;

• Parecer financeiro

• Aprovações

Abaixo um exemplo do formulário de solicitação de mudança.



Solicitação de mudanças Nº:

Nome do Requisitante:	Área Requisitante:	Data da Solicitação:
Nome do Projeto:		Prioridade:

Descrição da Solicitação

Motivo da Solicitação

Impactos Previstos

Escopo:
Custo:
Prazo:
Outros Impactos Previstos:

Documentos de referência

Anexos

Comitê Gestor

Parecer Técnico

Parecer Financeiro

Aprovações

Gestor:	Data:
Gestor:	Data:
Gestor:	Data:
Gestor:	Data:

por inadimplência da D'Gold; 10. GESTÃO DE MUDANÇAS Trata-se do processo de planejamen to e análise de impacto de mudanças no ambiente cibernético.

10.1. COMITÊ GESTOR DE MUDANÇAS

É composto por um gestor de cada área da D'Gold. Este grupo terá a responsabilidade de analisar e autorizar quaisquer mudanças no ambiente de tecnologia da informação.

10.2. SOLICITAÇÃO DE MUDANÇAS

Deverá ser preenchida pelo gestor da área requisitante. A solicitação deverá ser discutida em reunião do comitê. Ao final da análise deverão ser colhidas as assinaturas dos responsáveis, de acordo com a autoridade adequada.

10.3. FORMULÁRIO DE SOLICITAÇÃO DE MUDANÇAS

Este formulário deverá conter os seguintes itens:
a) Nome do Requisitante;

b) Área Requisitante;

c) Data da Solicitação;

d) Nome do Projeto;

e) Prioridade;

f) Descrição da Solicitação;

g) Motivo da Solicitação;

h) Descrição dos Impactos Previstos:
• Escopo
• Custo
• Prazo
• Outros Impactos

É importante ressaltar que caso a mudança solicitada seja a contratação de serviço na nuvem ou alteração contratual, deverá ser considerada a comunicação pelo menos com 60 dias de antecedência ao Banco Central do Brasil, e que todas as regras de contratação de serviços na nuvem constantes desta política sejam observadas.

i) Documentos de Referência;

j) Anexos;

k) Após a apreciação do Comitê Gestor deverão ser preenchidas as informações:
• Parecer técnico

11. DECLARAÇÃO DE RESPONSABILIDADE

Todos os administradores, funcionários, estagiários e prestadores de serviços regulares da F´DGOLD deverão aderir formalmente a está Política de Segurança Cibernética e assinar um Termo de Declaração de Responsabilidade, comprometendose a agir de acordo está Política de Segurança Cibernética.

12. MEDIDAS DISCIPLINARES

As violações a esta Política de Segurança Cibernética estarão sujeitas às sanções disciplinares e ou administrativas previstas nas normas internas da D´GOLD e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas

13. REVISÃO

A presente Política deverá ser objeto de revisão, no mínimo, a cada três anos, a contar da data de sua última revisão, ou a qualquer momento, na ocorrência de fato relevante ou mudanças na legislação aplicável.

14. AUDITORIA INTERNA

A Auditoria Interna da D'GOLD será responsável por recomendar melhorias contínuas nesta política através de processos de avaliação independente.
A Auditoria Interna responde diretamente ao Diretor Presidente da D'GOLD.

A Auditoria Interna executará revisões independentes para avaliar a efetividade da Política de Segurança Cibernética da D'GOLD, sempre de acordo com os requerimentos corporativos e regulatórios cabíveis com fins de informar sua opinião independente e recomendações para melhorias.

As atividades realizadas pela Auditoria Interna devem ser livres de interferências de qualquer tipo, incluindo seleção das auditorias, escopo, procedimentos, frequência, datas ou conteúdos reportados.