POLÍTICA INTERNA

DE SEGURANÇA CIBERNÉTICA

2023

Sumário

1. INTRODUÇÃO

O objetivo do presente documento é atender a Resolução nº 4.893/2021 do Banco Central do Brasil do Brasil e determinar as práticas a serem adotadas por todos os administradores, funcionários, estagiários e prestadores de serviços regulares da F.D'GOLD DTVM.

A informação é um dos principais bens de qualquer empresa, e a F.D'GOLD DTVM 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 F.D'GOLD DTVM 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.

O principal objetivo desta Política é assegurar a proteção dos ativos de informação da F.D'GOLD DTVM contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo de nossos negócios.

Esta Política está organizada de forma a dar pleno entendimento às determinações da referida Resolução, de acordo com os tópicos nomeados a seguir:

- Visão Geral;
- Política de Segurança Cibernética;
- Prevenção do Vazamento de Informações;
- Gestão de Riscos;
- Detecção de Intrusão;
- Proteção Contra Software Malicioso;
- Mecanismos de Rastreabilidade;
- Estratégia de Contingência ;
- Regras para Contratação de Serviços na Nuvem;
- Gestão de Mudanças.

2. VISÃO GERAL

O objetivo deste documento é determinar os objetivos, procedimentos e controles da F.D'GOLD DTVM que atendam aos requisitos da Resolução 4.893 de 26/02/2021.

O seu escopo refere-se à toda e qualquer informação acessada ou utilizada pelos administradores, colaboradores, 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 F.D'GOLD DTVM e está baseado em normas ISO consolidadas e nas boas práticas de mercado.
Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das Instituições Financeiras, permitindo assim agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros avanços.

Por outro lado, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas, hackers individuais, terroristas, colaboradores, competidores etc.) como por exemplo:

- Ganhos financeiros através de roubo, manipulação ou adulteração de informações;
- Obter vantagens competitivas e informações confidenciais de Clientes ou Instituições concorrentes;

- Fraudar, sabotar ou expor a Instituição invadida por motivos de vingança, ideias políticas ou sociais;
- Praticar o terror e disseminar pânico e caos;
- Enfrentar desafios e/ou ter adoração por hackers famosos.

As ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade e informações/bens de cada organização. As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além de riscos operacionais. Os possíveis impactos dependem também da rápida detecção e resposta após a identificação do ataque.

Tanto instituições grandes como menores podem ser impactadas e por esse motivo os ativos incorporados no espaço cibernético devem ser protegidos e preservados sendo também essa necessidade um dos motivos da implementação desta Política.

Entre esses ativos cibernéticos estão:

- Softwares, como um programa de computador;
- Conectividades como acesso à internet, Banco Central do Brasil, Receita Federal do Brasil, etc;
- Informações sigilosas de colaboradores;
- Componentes físicos, como servidores, estações de trabalho, notebooks e etc.

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores de mercado, incluindo o Banco Central do Brasil através da Resoluções nº 4.893/21 já mencionada, têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

3. OBJETIVO DA SEGURANÇA CIBERNÉTICA

A segurança cibernética tem como objetivo básico minimizar a vulnerabilidade da F.D'GOLD DTVM a incidentes de qualquer ordem, de modo a preservar suas informações confidenciais e garantir a continuidade de seus negócios.

Na abordagem da Resolução 4.893/21, a segurança cibernética está direcionada à contratação e execução de serviços na nuvem e devem prover:

- Rastreabilidade das informações sensíveis, com níveis de necessidade e confidencialidade determinados pelo responsável pela gestão;
- Registro, análise de impacto e o controle dos efeitos de eventuais incidentes;
- Assegurar a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) observadas as regras de sigilo e confidencialidade vigentes.
- Assegurar a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- Assegurar a disponibilidade dos dados e sistemas de informação utilizados na F.D'GOLD DTVM (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário).

A implementação desta Política considera as seguintes compatibilidades da F.D'GOLD DTVM:

- O porte, perfil de risco e o modelo de nossos negócios;
- A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais;
- A sensibilidade dos dados e das informações sob responsabilidade da instituição.

Os ambientes, sistemas, computadores e redes da F.D'GOLD DTVM poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Caberá a todos os colaboradores conhecer e adotar as disposições desta política e deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas ao exercício de suas atividades.

Conforme a Resolução nº 4.893/21, os serviços de computação em nuvem abrangem a disponibilidade da F.D'GOLD DTVM, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a F.D'GOLD DTVM implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos ou adquiridos;
- Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela F.D'GOLD DTVM utilizando recursos computacionais de seus prestadores de serviços;
- Execução por meio de Internet dos aplicativos implantados ou desenvolvidos por prestadores de serviços da F.D'GOLD DTVM, com utilização de recursos computacionais do próprio prestador de serviços contratado pela F.D'GOLD DTVM.

A F.D'GOLD DTVM é responsável pela Gestão dos serviços contratados incluindo as seguintes atividades:

- Análises de informações e de recursos adequados ao monitoramento dos serviços;
- Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a Prestadores de serviços;
- Cumprimento da legislação e da regulamentação vigente.

4. GESTÃO DE RISCO

Está sendo estabelecido um conjunto de medidas buscando mitigar os riscos de forma a impedir previamente a ocorrência de um ataque cibernético.

A F.D'GOLD DTVM oferece aos Colaboradores uma completa estrutura tecnológica para o exercício das atividades, sendo responsabilidade de cada Colaborador manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (Computador, notebook, acesso à internet, e-mail, etc.).

Equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da F.D'GOLD DTVM.

A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da F.D'GOLD DTVM depende de autorização do Diretor responsável pela Política de Segurança Cibernética devendo observar os direitos de propriedade intelectual pertinentes, tais como copyright, licenças e patentes.

As mensagens enviadas ou recebidas através do correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (internet) através de equipamentos da F.D'GOLD DTVM poderão ser monitoradas.

As senhas para acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.) compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa ou nome do departamento.

Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A segurança cibernética da F.D'GOLD DTVM contempla as seguintes ferramentas para a gestão de risco:

- Compliance;
- Classificação de Informações;
- Análise de Impacto;
- Plano de Contingências;
- Plano de Teste de Continuidade de Negócios.

5. 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 F.D'GOLD DTVM os seguintes mecanismos:

- Divulgação na Intranet;
- Treinamento e avaliação periódica;
- Divulgação junto aos clientes e usuários sobre as precauções no uso de produtos e serviços financeiros;
- Compromisso com alto nível de maturidade e com a melhoria contínua.

6. FUNDAMENTOS DA SEGURANÇA CIBERNÉTICA

É obrigação da F.D'GOLD DTVM 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:

- Controle de Acesso:
  - Do acesso ao local de trabalho;
  - Do acesso às dependências com valores monetários;
  - Do controle de acesso a sistemas de informação.
- Análise de Risco:
  - Plano de Contingências;
  - Normas de contratação de serviços.

Estes fundamentos estão baseados nas recomendações da Norma ISO 27002.

7. 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, colaboradores, estagiários e prestadores de serviços regulares da F.D'GOLD DTVM, 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.

7.1. 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:

- Manter acessos a sistemas e documentos protegidos por senhas não usuais;
- Imprimir relatórios;
- Anotar informações de forma manuscrita;
- Descartar informações na lata de lixo;
- Circular informações verbalmente, dentro e fora do ambiente da empresa.

7.2. 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.

7.2.1. 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, não podem ser repassados para outra pessoa interna ou externa à organização.

Ao identificar qualquer irregularidade nos recursos de tecnologia disponibilizados pela F.D'GOLD DTVM, o usuário deve comunicar imediatamente ao gestor da Política de Segurança Cibernética.

7.2.2. 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.

7.2.3. 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.

7.2.4. 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.

7.2.5. 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 F.D'GOLD DTVM.

7.2.6. Regras de uso da tecnologia

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

7.2.7. Comunicação

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

7.2.8. Conteúdo

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

7.2.9. Auditoria interna

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

7.2.10. 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.

7.2.11. Regras de uso do recurso computacional

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

7.2.12. Propriedade do recurso computacional

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

7.2.13. Disponibilização e uso

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

7.2.14. 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 F.D'GOLD DTVM poderá a qualquer momento retirar ou substituir o computador ou qualquer outro recurso computacional disponibilizado para qualquer usuário.

7.2.15. 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 F.D'GOLD DTVM.

7.2.16. 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).

7.2.17. Acesso ao recurso computacional

- 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;
- 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;
- É permitido apenas 5 tentativas máximas de autenticação de senha, sendo que na ocorrência de 5 tentativas malsucedidas, o acesso será automaticamente bloqueado;

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

7.2.18. Usabilidade de programas e aplicativos

- Os sistemas e programas básicos (sistema operacional e ferramentas) e componentes físicos serão implantados e configurados pela área de infraestrutura da Tecnologia (TI);
- É vedado aos usuários implantar novos programas e sistemas, ou alterar configurações sem a permissão formalizada da área de infraestrutura da Tecnologia (TI);
- É vedado aos usuários implantar ou alterar componentes físicos no computador ou em qualquer outro recurso computacional.

7.2.19. Histórico de verificação do computador e dos acessos

A F.D'GOLD DTVM manterá por 1 ano 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.

7.2.20. Responsabilidades do usuário

- Cuidar adequadamente do equipamento.
- O usuário é o custodiante deste recurso;
- Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de infraestrutura da Tecnologia (TI).

7.2.21. Outras proteções

- Será implementada o mecanismo de proteção de tela nos computadores e/ou proteção de ausência após 15 minutos de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente;
- Será implantado o "Hibernate" automático do sistema operacional por inatividade superior a 3 horas.

7.2.22. Termo de compromisso

Para ter acesso às informações da F.D'GOLD DTVM, o usuário deverá assinar (manual ou eletronicamente) um termo de compromisso. Os casos de exceção serão definidos pelo Comitê Gestor.

O departamento de Compliance da F.D'GOLD DTVM 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 F.D'GOLD DTVM 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.

7.3. Regras de uso da internet

7.3.1. Responsabilidade e forma de uso

O usuário é responsável por todo acesso realizado com a sua autenticação, 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 F.D'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 F.D'GOLD DTVM;
- 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;
- É proibido o uso de serviços de rádio, TV, download de vídeos, filmes e músicas, através dos computadores da F.D'GOLD DTVM, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pela área de infraestrutura da Tecnologia (TI);
- 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 F.D'GOLD DTVM.

7.4. Regras de uso do correio eletrônico corporativo (e-mail)

7.4.1. Endereço eletrônico do usuário

A F.D'GOLD DTVM disponibilizará endereços de seu correio eletrônico corporativo para utilização dos usuários no desempenho de suas funções profissionais. (ex.: usuario@dgold.com.br).

O endereço de correio eletrônico corporativo disponibilizado para o usuário é individual, intransferível, pertence à F.D'GOLD DTVM e deverá ser o mesmo durante todo o seu período de vínculo com a F.D'GOLD DTVM.

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.

7.4.2. 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 F.D'GOLD DTVM terão um limite máximo de armazenagem de dados de 50 GB e as mensagens enviadas/recebidas poderão conter arquivos anexos com até 20MB por mensagem.

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

7.4.4. Acesso à distância ou remoto

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

7.4.5. 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 F.D'GOLD DTVM.

Em situações autorizadas pela Diretoria, as mensagens do correio eletrônico corporativo de um usuário poderão ser acessadas pela F.D'GOLD DTVM 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.

7.4.6. Responsabilidades e forma de uso de correio eletrônico

O usuário que utiliza um endereço de correio eletrônico corporativo:

- É responsável por todo acesso, conteúdo de mensagens e uso relativos a este endereço de correio eletrônico corporativo;
- Poderá somente enviar mensagens necessárias para o desempenho de suas atividades profissionais na F.D'GOLD DTVM.

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 F.D'GOLD DTVM, 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 F.D'GOLD DTVM;
- Sejam incoerentes com o Código de Ética e Conduta;
- 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 F.D'GOLD DTVM;
- Deverá estar ciente de que uma mensagem de correio eletrônico corporativo da F.D'GOLD DTVM é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da F.D'GOLD DTVM;
- É proibido de emitir qualquer opinião pessoal, colocando-a em nome da F.D'GOLD DTVM, exceto quando especificamente autorizado para tal;
- Deverá observar se o endereço de correio eletrônico do destinatário corresponde realmente ao destinatário da mensagem desejado.

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.

7.5. Regras de uso do telefone

7.5.1. Número do telefone do usuário

A F.D'GOLD DTVM 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.

7.5.2. Propriedade do número do telefone

O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade exclusiva da F.D'GOLD DTVM.

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 F.D'GOLD DTVM 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.

7.5.3. 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 F.D'GOLD DTVM;
- 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 F.D'GOLD DTVM;
- Sejam incoerentes com o Código de Ética e Conduta da F.D'GOLD DTVM.

7.6. Classificação de informações sensíveis

Consiste no nível de acesso às informações geradas pelos sistemas da F.D'GOLD DTVM internamente ou de qualquer forma geradas ou recebidas pela F.D'GOLD DTVM.

A classificação passa a ser definida como:

- Restrito – Documento com acesso somente aos administradores da F.D'GOLD DTVM;
- Público – Documento com acesso livre;
- Secreto – Documento com acesso somente para a Diretoria da F.D'GOLD DTVM.

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 F.D'GOLD DTVM devidamente identificado.

As informações poderão constar da Intranet F.D'GOLD DTVM, desde que tenham o nível de divulgação devidamente classificado.

Deverá existir um índice indicando as informações existentes e as suas respectivas classificações de sigilo.

7.7. 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:

7.7.1. Identificação do risco

Informações de identificação do risco.

7.7.2. ID

Identificador do item de risco.

7.7.3. Data da identificação

Data da identificação do risco.

7.7.4. Risco

Denominação do risco;

7.7.5. Categoria

Categoria do risco. Pode ter os seguintes valores:

- Custo
- Escopo
- Prazo
- Qualidade

7.7.6. Probabilidade

Probabilidade de que o risco aconteça. Pode ter os seguintes valores:

- Alta
- Média
- Baixa

7.7.7. Impacto previsto

Tipo de impacto possível. Pode ter os seguintes valores:

- Alto
- Médio
- Baixo

7.7.8. Consequências

Descrição das consequências previstas caso o risco aconteça.

7.7.9. Exposição

Descrição do produto do impacto caso o risco aconteça.

7.7.10. Indicador

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

7.7.11. Valor de referência

Valor de referência para análise do indicador.

7.7.12. Resposta ao risco

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

7.7.13. Responsável

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

7.7.14. 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.

7.7.15. Estratégia para a ação

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

7.7.16. Data para a ação

Data prevista para a execução da ação.

7.7.17. Classificação do risco

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

7.7.18. Impacto

Tipo de impacto após a ação. Pode ter os seguintes valores:

- Alto;
- Médio;
- Baixo.

7.7.19. Situação

Descrição da situação após a ação.

7.8. Detecção de intrusão

O software nativo do firewall EDR (Endpoint Detection and Response), será responsável por detectar, prevenir e responder a ataques em tempo real. Ele oferece proteção contra ransomware, vírus, malware e outros programas cibernéticos perigosos.

O EDR deverá ser capaz de:

- Monitorar dispositivos de hardware do usuário;
- Detectar atividades e comportamentos suspeitos;
- Reagir automaticamente ao bloquear ameaças percebidas;
- Derrubar pacotes maliciosos;
- Bloquear o tráfego a partir do endereço de origem.

Como deverá estar o tempo todo on-line, EDR 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.

7.9. Proteção contra software malicioso

Os computadores da rede e os servidores na nuvem deverão estar protegidos por um software antivírus, 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).

7.10. Mecanismos de rastreabilidade

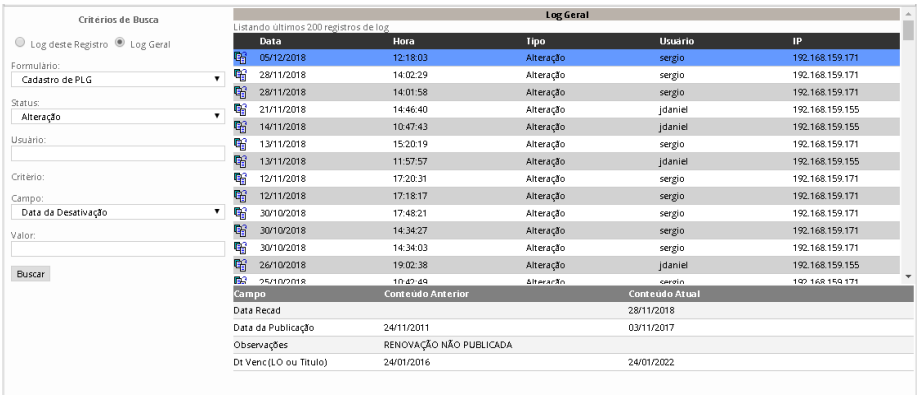
Para garantir a rastreabilidade dos processos executados pela F.D'GOLD DTVM, os seguintes instrumentos são utilizados:

7.11. 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:

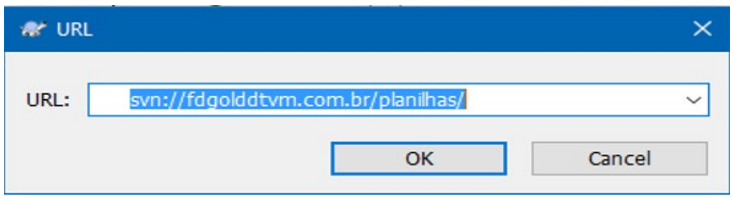


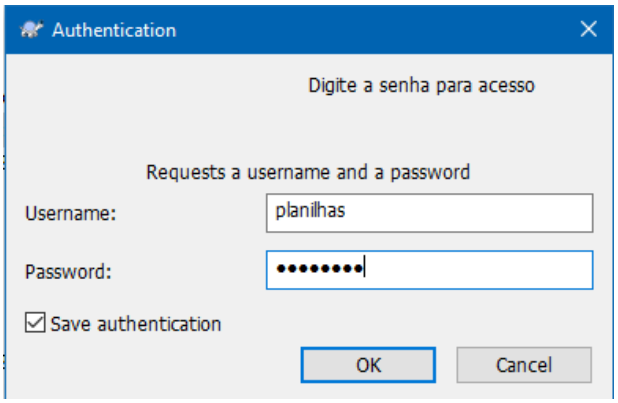
7.12. Arquivos de apoio (Planilhas, documentos e apresentações)

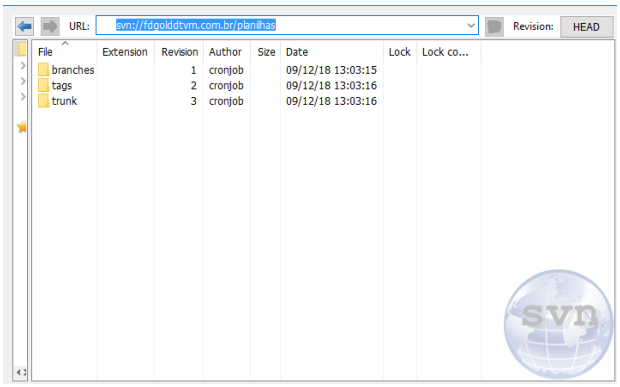
Os arquivos de apoio possuem repositório no servidor na nuvem, tendo suas versões controladas por um controle de repositório (SVN – Apache Subversion).

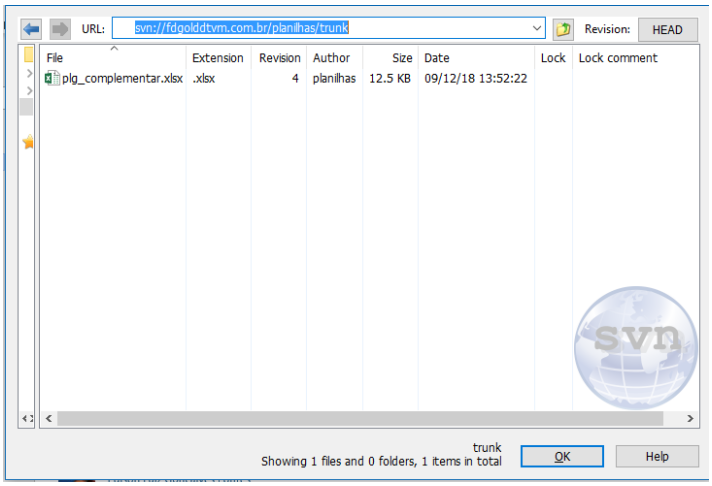
Cada usuário terá uma conta no SVN e deverá usá-la para baixar a última versão ou a versão desejada para a sua estação de trabalho.

Abaixo, um exemplo do uso do SVN:









7.13. Estratégia de contingência

A estratégia de contingência para o ambiente cibernético deverá conter:

7.13.1. Medidas de prevenção

Devem ser criados mecanismos de monitoramento de todas as ações de proteção implementadas para garantir o bom funcionamento e efetividade da segurança cibernética da F.D'GOLD DTVM através das seguintes ações:

- Manter inventários atualizados de hardware e software, bem como verificá-los com frequência para identificar elementos estranhos à instituição. Por exemplo, computadores não autorizados ou software não licenciado;
- Monitorar rotinas de backup, executando testes regulares de restauração dos dados;

- Realizar, periodicamente testes de invasão externa;
- Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura;
- 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);
- O plano de contingência deve prever ações no caso de incidentes na sede da F.D'GOLD DTVM ou nas empresas contratadas para armazenamento e processamento na nuvem, onde estarão hospedados os servidores;
- Para o caso de incidente na sede da F.D'GOLD DTVM, o plano de contingência deverá prever o novo local onde o negócio deverá ter continuidade;
- Um incidente na F.D'GOLD DTVM não alterará o funcionamento dos postos de compra de ouro bruto, em virtude de os servidores encontrarem-se na nuvem;
- Para o caso de incidente nos servidores, será restaurado um backup atualizado, e a restauração será comandada pela equipe de contingência da F.D'GOLD DTVM;
- Os dados armazenados nos servidores deverão ser restaurados com as cópias mais recentes dos backups, de forma a garantir imediata recuperação da atividade empresarial;
- Verificação periódica da disponibilidade e integridade dos dados nos servidores.
- Treinamento periódico dos colaboradores envolvidos com o plano de contingência;
- Plano de testes de continuidade de negócios;
- Testar o plano de resposta a incidentes, fazer os registros devidamente e documentação dos testes de continuidade de negócios com frequência mínima semestral.

7.13.2. Medidas de ação

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da F.D'GOLD DTVM, como por exemplo:

- Queda de energia elétrica;
- Falha de um elemento de conexão;
- Servidor fora do ar;
- Ausência de conexão com internet;
- Sabotagem / terrorismo;
- Indisponibilidade de acesso a F.D'GOLD DTVM;
- Ataques DDOS.

Deve-se seguir da seguinte forma:

a) Identificar o incidente;
b) Caso o incidente seja na sede da F.D'GOLD DTVM:
    - 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 F.D'GOLD DTVM, 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 de conexão para o endereço IP do servidor de contingência;
    - Testar o acesso dos usuários aos sistemas;

- Liberar a continuidade dos serviços.

Qualquer colaborador que detectar um incidente deverá comunicar imediatamente as demais áreas sobre o fato para que o mesmo seja levado ao conhecimento do Diretor responsável pela Política de Segurança Cibernética.

Visando a implementação das práticas da Política de Segurança Cibernética na F.D'GOLD DTVM, está implementando um Plano de Ação e de resposta a incidentes abrangendo o seguinte:

- As ações a serem desenvolvidas para adequar a estrutura organizacional e operacional aos princípios e diretrizes da Política de Segurança Cibernética;
- Os procedimentos, rotinas, controles e tecnologias a serem utilizadas na prevenção e na resposta a incidentes;
- Área responsável pelo registro e controle dos efeitos de incidentes relevantes.

O Plano de Ação e de Resposta a Incidentes será aprovado pelo Diretor responsável pela Política de Cibernética e será revisado no mínimo anualmente.

7.13.3. Incidente caracterizado

Caracterizado o incidente, devem ser tomadas as medidas imediatas, tais como:

- Iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de telefonia a desviar linhas de dados/e-mail, entre outros;
- O Diretor responsável pela Política de Segurança Cibernética estará avaliando o impacto do incidente nos diversos riscos envolvidos;
- Conforme a relevância (sabotagem, terrorismo, etc.) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providências;
- Conforme a relevância do incidente comunicar os envolvidos que por ventura tenham sido afetados;
- Comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pela F.D'GOLD DTVM.

7.14. Relatório sobre a implementação do plano de ação e resposta a incidentes

Será emitido anualmente, com data base de 31 de dezembro, relatório sobre a implementação do Plano de Ação e de Resposta a Incidentes.

Esse Relatório deve contemplar, no mínimo, as seguintes informações:

- A efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório deve ser elaborado até 31 de março do ano seguinte ao da data base devendo ser aprovado pelo Diretor responsável pela Segurança Cibernética.

7.14.1. Recuperação

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência de TI acionada e terceiros-chave notificados.

Quaisquer dados faltando ou corrompidos, ou problemas identificados por colaboradores internos devem ser comunicados à Diretoria.

7.14.2. Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

7.14.3. Justificativas para contratação de serviços na nuvem

A administração da F.D'GOLD DTVM, 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.

7.15. Parâmetros para contratação

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

- Comprovação se a empresa contratada possui Políticas de Segurança da Informação, plano de Continuidade Operacional, Gestão de Mudanças e Gestão de Incidentes;
- Comprovação de capacidade técnica levando em conta, inclusive, o potencial de crescimento da demanda;
- Comprovação de idoneidade e de cumprimento da legislação e da regulamentação vigentes;
- Que a F.D'GOLD DTVM tenha acesso garantido aos dados processados e/ou armazenados na empresa contratada;
- Garantia de confidencialidade, integridade, disponibilidade e recuperação dos dados processados e/ou armazenados na empresa contratada;
- Comprovação das certificações técnicas estabelecidas pela F.D'GOLD DTVM;
- Acesso da F.D'GOLD DTVM 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;
- Acesso às informações de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- Garantia da segregação dos dados dos clientes da F.D'GOLD DTVM;
- Garantia de qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da F.D'GOLD DTVM;
- No caso da execução de aplicativos por meio da internet, a F.D'GOLD DTVM deverá assegurar que o prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

A F.D'GOLD DTVM deverá possuir recursos e competências necessárias para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso de recursos.

7.16. Responsabilidades da F.D'GOLD DTVM

Na contratação dos serviços na nuvem são responsabilidades da F.D'GOLD DTVM:

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

- A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada pela F.D'GOLD DTVM ao Banco Central do Brasil, após 10 (dez) dias da contratação dos serviços, 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 após 10 (dez) dias da contratação dos serviços.
- 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 F.D'GOLD DTVM 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, devendo desenvolver iniciativas para compartilhamento de informações sobre os incidentes relevantes, bem como deixar essas informações compartilhadas disponíveis ao Banco Central do Brasil;
- A F.D'GOLD DTVM 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 F.D'GOLD DTVM deverá prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação destes serviços.

7.17. Itens dos contratos de prestação de serviços na nuvem

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

- 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;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes da F.D'GOLD DTVM;
- A obrigatoriedade, em caso de extinção do contrato, de:
    - transferência dos dados armazenados, processados ou gerenciados ao novo prestador de serviços ou à F.D'GOLD DTVM;
    - exclusão dos dados pela empresa contratada substituída, após a transferência e a confirmação da integridade e da disponibilidade dos dados recebidos pela nova empresa.
- Acesso da F.D'GOLD DTVM às informações prestadas na proposta de contratação, relativamente aos itens a e b;
- Informações comprovadas de certificações e relatórios de auditoria da prestadora de serviços;
- Informações comprovadas sobre os recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação de notificação à F.D'GOLD DTVM sobre a subcontratação de serviços relevantes relacionados ao objeto do contrato de prestação de serviços;
- 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;
- A adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil;

- A obrigação da prestadora de serviço em manter a F.D'GOLD DTVM permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;
- 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 da 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 por inadimplência da F.D'GOLD DTVM.

7.18. Gestão de mudanças

Trata-se do processo de planejamento e análise de impacto de mudanças no ambiente cibernético.

7.18.1. Comitê gestor de mudanças

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

7.18.2. 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.

7.18.3. 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.

Documentos de Referência:

i) Anexos;
j) Após a apreciação do Comitê Gestor deverão ser preenchidas as informações:
   - Parecer técnico
   - Parecer financeiro
   - Aprovações

7.19. Declaração de responsabilidade

Todos os administradores, funcionários, estagiários e prestadores de serviços regulares da F.D'GOLD DTVM deverão aderir formalmente a está Política de Segurança Cibernética e assinar um Termo de Declaração de Responsabilidade, comprometendo-se a agir de acordo está Política de Segurança Cibernética.

7.20. Medidas disciplinares

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

7.21. 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.

7.22. Auditoria interna

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

A Auditoria Interna executará revisões independentes para avaliar a efetividade da Política de Segurança Cibernética da F.D'GOLD DTVM, 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.

7.23. Documentos à disposição do banco central

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

- Política de Segurança Cibernética;
- Ata de Reunião da Diretoria da F.D'GOLD DTVM implementado a Política de Segurança Cibernética;
- Documento relativo ao Plano de Ação e de resposta a incidentes relativos à implementação da Política de Segurança Cibernética;
- Relatório anual sobre a implementação do Plano de ação e de resposta a incidente;
- Documentação sobre os procedimentos relativos à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem;
- Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, caso isso ocorra;

- Contratos de Prestação de serviços relevantes de processamento, armazenamento de dados e computação na nuvem;
- Dados, registros e informações relativas aos mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da política de segurança cibernética, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.