Política de Segurança

Sumário

Política de Segurança da Informação

1. Introdução

A Segurança da Informação visa preservar a confidencialidade, integridade e disponibilidade das informações utilizadas pela 3DB no desempenho de suas atividades, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte.

2. Abrangência

Esta política abrange todos os Colaboradores que tenham acesso à rede, informações confidenciais, computadores ou sistemas da 3DB.

3. Objetivo

A Política de Segurança da Informação ("Política") é o conjunto de diretrizes que objetiva proteger as informações da Sociedade, sejam elas, impressas, verbais e/ou sistêmicas, bem como o controle de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas estabelecem uma proteção adequada para qualquer empresa (ISO 27002).

4. Princípios

Os princípios básicos da Segurança da Informação são: confidencialidade, integridade e disponibilidade. Cada um deles denota uma postura diferente dentro da 3DB, exigindo ações pontuais para que se mantenham sempre presentes.

4.1. Confidencialidade

A confidencialidade, no contexto da segurança da informação, nada mais é do que a garantia de que determinada informação, fonte ou sistema é acessível apenas às pessoas previamente autorizadas a terem acesso.

4.2. Integridade

A integridade, no contexto da segurança da informação, visa a preservação da originalidade e confiabilidade das informações.

4.3. Disponibilidade

A relação da segurança da informação com a disponibilidade é basicamente a garantia de acesso aos dados sempre que necessário, possibilitando que os mesmos sejam acessados de maneira segura, rápida e eficiente.

5. Classificação da Informação

As informações que transitam pela 3DB são classificadas em quatro padrões distintos, conforme o disposto no Manual de Conduta e Ética (MACEQ) da Companhia, a saber: Informações Públicas, Informações Internas, Informações Confidenciais e Informações Restritas.

i. Informações Públicas: Aquelas destinadas a disseminação fora da 3DB. Possuem caráter informativo geral e são direcionadas ao público externo da 3DB. Exemplos: Código de Ética, normas divulgadas pelos Reguladores e Autorreguladores.

ii. Informações Internas: São aquelas destinadas ao uso dentro da 3DB. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente a 3DB ou seus Sócios e Colaboradores. Essas informações não exigem proteções especiais, salvo aquelas entendidas como mínimas para impedir a divulgação externa não intencional. Exemplo: normas e políticas internas.

iii. Informações Confidenciais: Também se destinam ao uso interno da 3DB. Entretanto, se diferem das informações de natureza interna, na medida em que sua eventual divulgação poderia afetar significativamente os negócios da 3DB, seus Sócios e Colaboradores. Exemplos: registros de empregados, planos salariais e informações sobre os Sócios. Sua divulgação é proibida, salvo se solicitada pelo órgão fiscalizador competente, situação na qual deverá ser prestada, mediante autorização da Diretoria ou da área de Compliance. Exemplos: informações sobre os negócios, pesquisas, planos de novos negócios, estratégias, registros, bancos de dados, informações sobre salários e benefícios, dados médicos de Colaboradores.

iv. Informações Restritas: Correspondem as informações cuja divulgação não autorizada provavelmente provocaria danos substanciais, constrangimentos e/ou penalidades a 3DB, seus Sócios, e/ou colaboradores. Consideram-se informações de

natureza confidencial todas as informações às quais os Colaboradores venham a ter acesso, em decorrência do desempenho de suas funções na 3DB, inclusive por meio dos sistemas e arquivos disponibilizados para tanto, que não sejam notória e comprovadamente de domínio público. As pessoas designadas para o trato e uso de tais informações têm a responsabilidade de garantir que elas sejam devidamente protegidas e seguramente armazenadas quando não estiverem em uso.

Na ocorrência de dúvidas sobre o caráter de confidencialidade de qualquer informação, o colaborador deve, previamente à sua divulgação, consultar o responsável pela área de Compliance para obter orientação adequada, o qual deverá atribuir interpretação extensiva ao conceito de informação confidencial definido acima, conforme orientação disposta no Manual de Conduta e Ética (MACEQ) da 3DB.

6. Uso do E-mail

Como se trata de ferramenta de trabalho, o e-mail poderá ser rastreado, monitorado, gravado e/ou inspecionado, sem prévio aviso, com objetivo de evitar riscos decorrentes de ataques externos e do mau uso da ferramenta. Os Colaboradores, com a aceitação dos termos e condições das Políticas da 3DB, estão cientes de que as informações transmitidas e recebidas em sua conta de e-mail poderão ser monitoradas pela 3DB, ficando cientes de que o uso indevido ou não autorizado os sujeitará a punições. A 3DB se reserva o direito de controlar e monitorar seus conteúdos e formas de utilização.

7. Gravação Telefônica

A Central Telefônica registra todas as ligações recebidas e efetuadas de todos os ramais e linhas instaladas, no entanto, em função de obrigatoriedade normativa, algumas áreas da 3DB podem ter seus ramais ligados a sistema de gravação de voz. Estas gravações serão verificadas quando necessário pelo Compliance. A escuta por qualquer funcionário só poderá ser realizada com a aprovação desta área ou seus Diretores.

As áreas que mantem sistemas de gravação ativos são: Atendimento técnico, Atendimento comercial e Atendimento Administrativo/Financeiro.

8. Política de senhas e direito de acesso à rede e e-mail

8.1. Senhas

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos.

Todos os computadores da 3DB possuem senhas de acesso individuais e intransferíveis que permitem identificar o seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

As senhas são de caráter sigiloso, pessoal e intransferível e serão fornecidas aos Colaboradores da 3DB. Em nenhuma hipótese as senhas deverão ser transmitidas a terceiros.

A troca de informações entre os Colaboradores da 3DB deve sempre pautar-se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida, solicitar esclarecimento por e-mail ao gestor imediato, antes da revelação.

Os usuários e senhas de login na rede são cadastrados e gerenciados pelo aplicativo Active Directory da Microsoft, de modo a controlar o acesso a pastas e arquivos da 3DB. Tais senhas deverão trocadas a cada 45 (quarenta e cinco) dias, por imposição das políticas de segurança. Os e-mails são controlados pelos software Zimbra onde são cadastrados os Colaboradores da 3DB conforme solicitação do “RH” para as áreas Técnica, Administrativa e Comercial.

8.2. Acesso ao cliente

Toda a comunicação entre o ambiente do cliente e da 3DB é feito através de um túnel criptografado, utilizando chaves únicas.

8.3. Controle de Acesso

O controle do acesso ao cliente é feito através de ferramenta de mercado, tal ferramenta armazena de forma segura a senha de acesso do cliente e cada colaborador através de seu usuário Active Directory tem acesso aos recursos do cliente sem ter acesso a senha do cliente para execução de suas atividades diárias. O acesso deverá ser liberado ao colaborador de acordo com seu nível de atendimento (Ex.: N1 Infra tem acesso a estações de trabalho, N3 Infra tem acesso a Servidores AD, DBA tem acesso aos Bancos de Dados).

8.4. Rastreabilidade

Todo o acesso a cliente é registrado, gerando assim, trilha de auditoria de todas as sessões criadas. Dessa forma para os sistemas operacionais Linux são gravados todos os comandos executados em formato texto e feita a gravação da tela. Para os sistemas Windows o acesso é realizado através do protocolo RDP e todas as sessões são gravadas e armazenadas por 90 dias.

8.5. Armazenamento e acesso as senhas

Quaisquer senhas que a 3DB tenha acesso ficam armazenadas em um cofre (Sistema de Senhas), criptografado, disponível exclusivamente através da nossa VPN. Somente usuários privilegiados e que necessitem ter acesso ao cofre têm essa concessão.

Quando o Colaborador da 3DB é desligado, imediatamente através de comunicação do RH, o seu acesso a todos os sistemas da 3DB (sistemas internos, e-mail, Intranet, pastas e arquivos da rede, etc.) será bloqueado.

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

As senhas são criadas pelos usuários respeitando as políticas de administração de rede, controlada através da ferramenta Microsoft Active Directory:

- Recomendações:
  - Mínimo de 8 caracteres;
  - Utilize alguma regra para criar sua senha e memorizar;
  - Troque letras por números ou caracteres especiais. Por exemplo i=1, s=5, a=4, t=7, o=0;
  - Utilize as duas mãos para criar/digitar sua senha.

- Exemplo do que não é recomendado:
  - Senhas sequenciais: 1234, 4321, senha123, etc.;
  - Nomes de parentes;
  - Placas de carros;
  - Palavras utilizadas no ambiente de trabalho, comum à sua atividade;
  - Não utilize a opção “Lembrar senha” em computadores públicos.

8.6. Mesa Limpa

É recomendável aos Colaboradores da 3DB nunca deixar documentos expostos nas mesas. Sendo assim, orienta-se para sempre que o usuário sair do seu posto de trabalho, levar consigo ou guardar/arquivar os documentos que eventualmente estejam nas mesas para que outros não tenham acesso às informações confidenciais.

É recomendado também, que o Colaborador antes de ir embora no fim do expediente, não deixe nenhum documento sobre a mesa, mantendo os documentos do dia a dia, arquivados em armários/gaveteiros trancados.

8.7. Sistemas

Colaboradores da 3DB terão acesso ao sistema, conforme cadastro efetuado pela área de Recursos Humanos ("RH") ou Administrativo quando PJ. Quando o Colaborador da 3DB é desligado, imediatamente através de comunicação do RH ou Administrativo, é bloqueado o seu acesso a todos os sistemas da 3DB (sistema aplicativo, e-mail, Intranet, pastas e arquivos da rede, etc.) conforme mencionado no item 8.5.

O acesso ao sistema se dará por um dos computadores ligados a rede corporativa ou através de conexão criptografada VPN, por acesso remoto. Utilizamos as credenciais já citadas do Active Directory para controlar este acesso e após esta primeira autenticação, é liberado acesso ao ícone para acesso ao ERP. Deverá a partir deste ponto utilizar as credenciais fornecidas após o cadastro.

8.8. Diretórios

O uso da rede para armazenar os arquivos pessoais é permitido, desde que a pasta seja corretamente identificada, ficando o colaborador ciente de que não será assegurada privacidade às informações armazenadas, as quais poderão ser acessadas por quaisquer Colaboradores que possuam acesso à rede.

Os colaboradores possuem acesso a pasta padrão de cada departamento, dependendo de solicitação formal para o acesso a subpastas restritas as equipes. As solicitações de acessos aos diretórios deverão ser formalizadas ao gestor de cada área.

Os acessos serão concedidos após autorização formal, por e-mail do gestor do departamento responsável pela área de diretórios solicitada.

O controle de permissões é feito pelo Active Directory/OneDrive, conforme já mencionado.

8.9. Acesso ao USB

O acesso a dispositivos via porta USB é limitado a leitura das informações. Não é permitido a escrita ou edição do conteúdo, em nenhum computador da 3DB, independente do dispositivo conectado sem autorização prévia do Gestor.

8.10. Acesso a rede via WI-FI

O acesso à rede interna via Wi-Fi é permitido para todos os colaboradores.

A rede Wi-Fi "3DB Visitantes" é liberado a todos os colaboradores da 3DB usando dispositivos pessoais e visitantes da 3DB. Esta rede permite acesso apenas a internet e serviços nela disponível. O acesso é restrito a sites pertinentes ao ambiente corporativo, ou seja, conforme item 8.11 Internet.

Os acessos, mesmo pela rede de convidados, podem ser monitorados e controlados.

Não é permitido através da rede Wi-Fi "3DB Visitantes" o acesso à rede de computadores da corporação e por sua vez, Data Center, sistemas internos e servidores.

A rede Wi-Fi "3DB Solutions" provê acesso à rede de computadores da corporação e por sua vez, Data Center, sistemas internos e servidores. Por isso é restrito/exclusivo a colaboradores da 3DB, com controle de senhas e permissões já descritos acima.

O acesso a rede Wi-Fi "3DB Solutions" não deve ser fornecido a visitantes, fornecedores e/ou pessoas que não faça parte da 3DB.

8.11. Internet

Os Colaboradores deverão utilizar os recursos de acesso à internet apenas para assuntos corporativos, sendo a utilização para fins particulares tratadas como

exceção. Para preservar esses recursos, a 3DB se reserva o direito de controlar e monitorar seus conteúdos e formas de utilização.

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

i. não é permitido visitar sites na internet que contenham materiais obscenos, lascivos, preconceituosos ou outro tipo de material repreensível;
ii. não é permitido enviar ou receber material obsceno ou difamatório ou cujo objetivo seja aborrecer, assediar ou intimidar terceiros;
iii. não é permitido utilizar os computadores da Sociedade objetivando práticos de atos ilícitos;
iv. não é permitido apresentar opiniões pessoais como se fossem da 3DB.

É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, atividades de hacker e quaisquer outras atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento da área de Tecnologia, Diretoria ou Compliance.

Utilizamos um equipamento do tipo “Next Generation Firewall”, que realiza o controle de acesso a aplicações e sites, conforme descrição. Este equipamento realiza o registro do log de acesso e bloqueio, ficando disponível por um período de 6 meses.

8.12. Política de Backup

Todos os documentos arquivados pelos colaboradores na rede, ou seja, nos servidores são objeto de back-up diário com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

O backup é feito diariamente via recurso da Cloud Oracle e é armazenado backups diários por uma semana, backups semanais por 4 semanas, mensais por 12 meses e anuais por 5 anos.

8.13. Estrutura da Rede

Atualmente, temos 1 escritório conectado por link de internet via VPN criptografada a Cloud Oracle utilizando equipamentos do tipo “Next Generation Firewall”.

Utilizamos o data center ORACLE Cloud, sendo São Paulo nosso site principal, utilizamos todos os recursos de nuvem para ter alta disponibilidade dos serviços e backup como descrito acima.

A nuvem pública da Oracle (OCI), que possui as seguintes certificações de segurança:

CSA Star Level 1

- EU Model Clauses
- GDPR—General Data Protection Regulation
- ISO/IEC 27001:2013—International Organization for Standardization 27001
- PCI DSS—Payment Card Industry Data Security Standard
- SOC 1—System and Organization Controls 1
- SOC 2—System and Organization Controls 2
- TISAX

Que podem ser consultadas aqui: https://www.oracle.com/br/cloud/cloud-infrastructure-compliance/

Toda a comunicação é criptografada entre o escritório e os data centers, e os controles de acesso à rede, e-mail, sistema, intranet, pastas de arquivos, internet, etc, são controlados pelos meios informados anteriormente, sempre com as mesmas políticas.

8.14. Software e Computadores

Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo gestor de cada área.

Downloads de qualquer natureza devem ser realizados de sites confiáveis. Os sites de downloads conhecidos são bloqueados, não sendo permitido a baixa de softwares, com exceção a softwares do governo, desde que de forma justificada. Periodicamente e sem aviso prévio, poderão serão realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

A cópia de arquivos e instalação de programas em computadores, será executada apenas com as credenciais da equipe de Infra da 3DB, bem como deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

Todo o sistema eletrônico utilizado pela 3DB está sujeito à revisão, monitoramento e gravação a qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

A aquisição de computadores é feita sempre pela equipe de infra, com o intermédio do financeiro e com a autorização da Diretoria Administrativa. Normalmente, a compra é feita em uma empresa especializada em tecnologia, considerada uma das principais fornecedoras de Hardware.

A cotação e compra de softwares, normalmente, ocorre com a mesma empresa de tecnologia mencionada no parágrafo acima, pois a mesma possui grande

representatividade junto aos maiores de software. As compras são realizadas com descontos ou parcelamentos em cartão de crédito.

Para troca de computadores é feita avaliação do desempenho e se este não atende mais a função do colaborador, ou se possui algum software OEM (comparado junto com a máquina) que representa algum risco a segurança da informação, deverá ser substituído, tendo em vista que nesses casos, não há suporte do fabricante.

8.15. Vírus

Nos computadores e servidores da 3DB é utilizado o software padrão de antivírus do Windows como solução antivírus. Tal software não possui renovação de licença de uso e suporte anual junto ao fabricante.

A atualização das definições de vírus é realizada de forma automática, pelo menos uma vez por dia. Esta definição é enviada a todos os computadores e servidores e garante que os vírus “lançados” mais recentemente sejam detectados e removidos. Além destas definições, esta ferramenta possui módulo de detecção de comportamento, o que permite que um vírus ou software malicioso, mesmo não mapeado pelo fabricante seja bloqueado e eliminado.

A detecção de vírus é monitorada automaticamente pelo software antivírus, sendo assim, no caso da detecção de vírus no computador, o usuário, a princípio, não precisa realizar nenhuma interação com software. Posteriormente, a área de TI monitora as ações tomadas pelo software.

São realizadas semanalmente ações proativas para detecção de falhas da ferramenta e, se necessário atualização ou reinstalação, garantindo que nenhum computador ou servidor fique sem o software em pleno funcionamento.

Temos em nosso firewall e AntiSpam um módulo de detecção de vírus, “spyware e ransonware”, sendo assim, caso ocorra a tentativa de recebimento ou download de algum item malicioso, o bloqueio e a comunicação a área de TI, se darão automaticamente. Outro módulo em nosso firewall é o IPS, que trabalha na prevenção de intrusões, seja por ferramentas ou manualmente.

8.16. Patrimônio

É de responsabilidade de todos os Colaboradores a utilização responsável, a conservação e a proteção dos patrimônios da 3DB, contra perda, roubo e mau uso.

Por patrimônios entende-se todos os equipamentos (telefones, celulares, computadores, notebooks, etc...) e recursos eletrônicos, bem como tecnologias, estudos e planos de desenvolvimento de negócios, produzidos pelos Colaboradores ou colocados à sua disposição pela Sociedade com a intenção de propiciar as ferramentas e informações necessárias ao desempenho da função e que incentivem a eficiência de cada Colaborador.

O patrimônio da Sociedade deverá ser utilizado exclusivamente para a consecução do seu objeto social, sendo dever de todos os Colaboradores a sua preservação e utilização adequada.

9. Plano de continuidade de negócios

O plano de Continuidade de Negócios da Sociedade consiste no uso de sistemas na nuvem e equipamentos em ambiente alternativo, facilitando o deslocamento para outros sites, caso necessário.

O processo de Continuidade de Negócio estabelece as estruturas de proteção e os procedimentos operacionais em situação emergencial em casos de incidência de falhas/indisponibilidade dos recursos existentes.

Temos como contingência a possibilidade de trabalho na modalidade “home office”, onde o colaborador tem acesso via VPN Corporativa a todos os recursos de rede e sistema da 3DB conforme seu nível de acesso para desempenhar suas atividades diárias sem a necessidade de estar na sede da empresa.

Para contingência de nosso data center principal, temos replicação dos arquivos e bancos de dados e sistemas para o site de DR (Disaster Recovery), conforme mencionado no item 8.13. O acionamento deste site é feito caso decretando o desastre no site principal. Toda a ativação do site de desastre deverá ser acompanhada pela equipe de Infra para as devidas configurações.

São realizados testes semestrais para ambos ambientes, validando o plano e corrigindo eventuais falhas ou documentando novas demandas.

10. Política de segurança cibernética

10.1. Avaliação de riscos, correções e mitigação de falhas

Semestralmente a 3DB contrata empresas especializadas em testes de intrusão, avaliação de ambiente e detecção de riscos no ambiente de TI. Esta avaliação completa é acompanhada pela equipe de Segurança da 3DB.

O documento final desta avaliação é um detalhamento de todos os problemas, falhas e riscos encontrados, bem como as devidas soluções.

Com base neste documento é realizado um planejamento para correção dos problemas ou mitigação no caso de problemas encontrados, mas sem solução ou suporte pelo fabricante. Podemos optar inclusive pela migração do serviço caso não exista uma solução definitiva à falha.

Estas empresas especializadas em segurança da informação, bem como a consultoria que temos contrato firmado, são responsáveis por apontar novas descobertas de falhas, conforme boletim informativo dos fabricantes ou empresas especializadas, em itens utilizados em nosso ambiente.

As ações para correção serão tomadas assim que publicada as ferramentas para isso e até lá são decididas ações para mitigação.

10.2. Contratação de terceiros

Empresas contratadas para serviço terceirizado são obrigadas a utilizar conexão criptografada "VPN" para realização de suas atividades. Todas as regras de segurança mencionadas são aplicadas aos terceiros, além da assinatura de NDA e devido contrato de prestação de serviço, de acordo com o objeto.

Os usuários criados para estas empresas, são nominais e limitados ao escopo do contrato firmado, ou seja, não terão acesso amplo ao ambiente, podendo ficar restrito apenas a um determinado servidor ou estação de trabalho para que possa realizar sua atividade.

10.3. Identificação de novos riscos

A 3DB conta com ferramentas como o Antivírus, Firewall com IPS e IDS e AntiSpam que geram relatórios automáticos contendo informação de riscos do ambiente, podendo inclusive identificar tentativa de acesso ou comportamento de usuário e serviço potencialmente perigoso. A partir daí a equipe de TI avalia qual a real necessidade e qual ação deverá ser tomada.

10.4. Plano de respostas a incidentes

Para elaboração de planos de respostas a incidentes, temos estabelecido como política a manutenção e atualização mínima mensal, ou sempre que houver movimentação, atualização ou novas instalações em nossa estrutura, conforme segue:

- Lista de Fabricantes de hardware instalados;
- Lista Fabricantes de softwares instalados;
- Inventário de estações de trabalho;
- Inventário de servidores físicos e virtuais com seus respectivos serviços;

- Diagrama de rede;
- Estrutura organizacional da empresa; e
- Lista de contratos com empresas terceirizadas, com seus contatos de emergência e scalation list caso exista.

Esta documentação pode ser feita em sistemas especialistas ou documentos eletrônicos como word e excel, disponibilizado nos diretórios de rede.

O Gestor de Atendimento, mais os colaboradores analistas de Infra, Segurança e Banco de Daos e nossas consultorias (com contratos firmados) como apoio, compõem a equipe responsável a dar as respostas aos incidentes.

Em caso de crise, são participados membros da diretoria e presidência para decidir ações a fim de impactar o mínimo possível os negócios.

11. Controle de revisões da política de segurança

Revisão da Política	Data	Motivo
Sebastião Santos	Julho, 2020	Criação