JBCred S.A. Sociedade de Crédito, Financiamento e Investimento

Políticas de Cyber-Segurança da Informação e Utilização de Recursos da Rede

---
Wagner Caetano - Gestor de TI - JBCRED

Elaine Gois – Diretor Responsável por TI perante o BCB

Maio
2024

1 Introdução

Com a grande utilização da Internet nascem as preocupações diretamente ligadas aos dados/informações da JBCRED. Sendo assim com o avanço da utilização desta ferramenta faz-se necessário a definição de um política interna que defina normas e diretrizes para a Segurança da Informação. Estas normas estarão disponíveis e divulgadas na intranet para garantir a integridade, confidencialidade e disponibilidade das informações sob responsabilidade da JBCRED.

Segundo a Norma ISO/IEC 27002 a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é essencialmente importante no ambiente de negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças a vulnerabilidades.

As informações contidas na Política de Segurança, irão descrever as normas de utilização e as atividades que violam o bom uso dos serviços disponibilizados pela JBCRED, as quais são consideradas proibidas.

Estas Normas devem ser divulgadas para todos os funcionários da instituição e obedecidas por todos que utilizam os recursos e serviços disponibilizados sendo de responsabilidade de cada um o seu cumprimento. A Política estará disponível no endereço http://www.jbcred.com.br/intranet - Intranet da JBCRED. O cumprimento desta Política de Segurança será acompanhado e auditado pelo setor de TI da JBCRED.

A instituição, mediante autorização expressa da alta direção, se reserva o direito de monitorar, automaticamente, a estação de trabalho, o tráfego efetuado através das redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico.

A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas.

Este documento será revisado todo ano, ou a qualquer momento quando a segurança da rede assim o exigir.

2 Termos e Definições

Para os efeitos desta Política, aplicam-se os seguintes termos e definições:

Ativo: qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004].

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.
Nota: Controle é também usado como um sinônimo para proteção ou contramedida.

Diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas. [ISO/IEC 13335-1:2004].

Recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.
Segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falta de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Incidente de segurança da informação: indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004].

Política: intenções e diretrizes globais formalmente expressas pela direção.

Risco: combinação da probabilidade de um evento e de suas consequências [ABNT ISSO/IEC Guia 73:2005].

Análise de riscos: uso sistemático de informações para identificar fontes e estimar riscos [ABNT ISSO/IEC Guia 73:2005].

Análise/avaliação de riscos: processo completo de análise e avaliação de riscos [ABNT ISO/IEC Guia 73:2005].

Avaliação de riscos: processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco [ABNT ISSO/IEC Guia 73:2005].

Gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos [ABNT ISSO/IEC Guia 73:2005].

Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco [ABNT ISSO/IEC Guia 73:2005].

Terceira parte: pessoa ou organismo reconhecido como independente das partes envolvidas, no que se refere a um dado assunto [ABNT ISO/IEC Guia 2:1998].

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. [ISO/IEC 13335-1:2004].

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. [ABNT NBR ISO/IEC 27002:2005].

3 Objetivos

Este documento tem como objetivo dispor sobre a política de disponibilização e utilização dos recursos de tecnologia da informação no âmbito da JBCRED S/A SOCIEDADE DE CRÉDITO, FINANCIAMENTO E INVESTIMENTO. Também são objetivos da política de segurança definida neste documento:

- Estabelecer regras para a disponibilização e utilização de serviços de rede de dados, internet, telecomunicações e correio eletrônico institucional.
- Aprovar as políticas, normas e procedimentos de segurança da informação.
- Designar, definir ou alterar as responsabilidades da área de Segurança da Informação.
- Aprovar novos controle ou alterar as responsabilidades da área de Segurança da Informação.
- Apoiar a implantação de soluções para a minimização dos riscos.
- Dar suporte às iniciativas na área de Segurança da Informação.

4 Considerações Gerais

Este documento foi desenvolvido para assegurar que os usuários que utilizam diretamente ou indiretamente recursos computacionais, serviços de internet, rede de dados, telefonia e e-mail providos pela JBCRED S/A SOCIEDADE DE CRÉDITO, FINANCIAMENTO E INVESTIMENTO possam fazer o uso consciente e responsável dos mesmos.

A JBCRED se reserva ao direito de utilizar ferramentas e técnicas que auxiliam no monitoramento, controle e armazenamento de registros de acesso de conteúdo de quaisquer formas de comunicação que se utilizem da infraestrutura provida pela empresa.

Todo e qualquer acesso à rede local e internet deverá ser feita através de um login de acesso único, pessoal e intransferível que será disponibilizado pelo setor de TI.

5 Responsabilidades e Proibições

A responsabilidade pela segurança das informações estará estabelecida na Política de Segurança da Informação.

O monitoramento do uso da internet se torna importante para que todos os acessos dos usuários sejam registrados e para que os mesmos possam ser notificados e até punidos no caso de acesso que sejam contrários a política da empresa.

Para fins de auditoria e controle para comprovação dos acessos são necessários o armazenamento das informações juntamente com os sites utilizados. Os dados mais críticos a serem armazenados para possível auditoria futura são: identificação do usuário, data e hora de conexão, endereço de IP de origem, protocolos utilizados e logs de servidores que devem ser armazenados pelo período de 12 meses.

São responsabilidades dos usuários de serviço de dados, internet, telecomunicações, e-mail e recursos computacionais da JBCRED:

- Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de suas respectivas senhas.
- Seguir de forma colaborativa as orientações fornecidas pelo departamento de TI em relação ao melhor uso dos recursos computacionais, de rede de dados, internet, telecomunicações e e-mail.
- Efetuar cópias de segurança de seus arquivos, catálogos de endereço, e-mails e quaisquer outros materiais de ordem digital.
- Utilizar de forma ética e legal os recursos computacionais, de rede de dados, internet, telecomunicações e e-mail.
- Não alterar configurações dos softwares de segurança como antivírus e firewall.

São proibições dos usuários de serviço de dados, internet, telecomunicações, e-mail e recursos computacionais da JBCRED:

- Utilizar dos meios e recursos de comunicações da JBCRED para difamar, prejudicar, subtrair, caluniar ou molestar outras pessoas ou instituições.
- Utilizar, examinar, copiar, armazenar, distribuir ou instalar programas ou qualquer material que seja protegido por direito autoral.
- Utilizar dos meios e recursos de comunicações da JBCRED para campanhas políticas e ou propagandas comerciais.
- Tentar ou Violar qualquer sistema de segurança da JBCRED ou de qualquer outra instituição ou pessoa.
- Efetuar ou tentar qualquer tipo de acesso não autorizado a dados da empresa ou de qualquer outra instituição ou pessoa.
- Fazer-se passar por outra pessoa ou dissimular sua identidade quando utilizar qualquer meio ou recurso da empresa.
- Transmitir, difundir ou disponibilizar a terceiros, informações, dados, conteúdos, mensagens, gráficos, desenhos, arquivos e som e/ou imagem, fotografias, gravações, software ou qualquer classe de material que, de qualquer forma, induzam, incitem ou promovam atos ilegais, denegridores, difamatórios, infames, violentou e ou, em geral contrários à lei, à moral e aos bons costumes geralmente aceitos ou à ordem pública.
- Transmitir, difundir ou disponibilizar a terceiros informações e dados pertencentes a JBCRED.

6 Política de Cadastros e Senhas

Uma senha (password) na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, é utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser.

Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você na Internet ou na Rede Local. Alguns dos motivos pelos quais uma pessoa poderia utilizar sua senha são:

- Ler e enviar e-mails em seu nome.
- Obter informações sensíveis dos dados armazenados em seu computador, tais como números de cartões de crédito.
- Esconder sua real identidade e então desferir ataques contra computadores de terceiros.

Portanto, a senha merece consideração especial, pois ela é de sua inteira responsabilidade.

A Gerência Administrativa é o setor responsável por solicitar o cadastramento ou exclusão de funcionários e colaboradores, devendo proceder ao registro das informações básicas dos mesmos. Em caso de desligamento do funcionário ou colaborador, caberá à Gerência Administrativa a imediata solicitação de exclusão do acesso do mesmo. A Gerência Administrativa deverá proceder a coleta das informações básicas do colaborador para confecção do cadastro.

O cadastramento da senha será realizado pela Gerência Técnica, a qual fornecerá o nome de usuário e senha inicial ao funcionário ou colaborador por e-mail alternativo ou telefone. A senha inicial é uma senha padrão e deverá ser modificada pelo colaborador logo no primeiro acesso respeitando a política de senhas adotada pela JBCRED. Esta senha tem um prazo de validade de 3 meses e sempre deverá ser renovada por outra ainda não utilizada.

A senha é de total responsabilidade do colaborador, sendo terminantemente proibida sua divulgação ou empréstimo a qualquer outra pessoa, nem mesmo da Gerência Técnica, devendo a mesma ser alterada imediatamente no caso de suspeita de sua divulgação.

Em caso de esquecimento ou bloqueio de senha, o funcionário ou colaborador deverá entrar em contato com a Gerência Técnica que irá confirmar algumas informações de cadastro, zerar a senha para a senha padrão e fornecê-la ao solicitante para que no acesso subsequente seja ele possa cadastra uma nova senha de acesso.

Qualquer ato praticado com a utilização da senha será responsabilidade do seu respectivo colaborador. Não será aceita alegação de que outra pessoa utilizou algum recurso com a senha do colaborador.

7 Política de utilização de Internet

A internet é uma grande fonte de informações e a mais poderosa ferramenta de trabalho atual. Por estes motivos ela deve ser considerada quando utilizada dentro da empresa, em horário de expediente: como ferramenta de trabalho.

A JBCRED disponibilizará acesso à internet aos funcionários e colaboradores que necessitem deste recurso para execução de suas tarefas, ficando o funcionário responsável pelos acessos registrados em sua sessão de conexão.

É proibido, ao funcionário e colaborador, a utilização do acesso à internet para fins ilícitos. A JBCRED adotará mecanismos para evitar a utilização para estes fins, estando o colaborador ciente de que é o único responsável pelos atos praticados na Internet.

Visando a otimização dos canais de acesso à internet, a proteção contra ataques de vírus e hackers e, ainda, o aumento da produtividade dos colaboradores, é vedada a utilização do acesso à internet para os seguintes fins:

- É proibido utilizar os recursos da empresa para fazer o download ou distribuição de software ou dados não legalizados;
- É proibido a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
- Poderá ser utilizada a Internet para atividades não relacionadas com os negócios durante o horário de almoço, ou fora do expediente, desde que dentro das regras definidas pela JBCRED;
- Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;
- Funcionários com acesso à Internet não podem efetuar upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados;
- Caso a empresa julgue necessário haverá bloqueios de acesso à arquivos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos e domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos;
- Haverá geração de relatórios dos sites acessados por usuário e se necessário a publicação desse relatório;
- Utilização ou acesso de programas de rede P2P para compartilhamento de arquivos, músicas ou vídeos;
- Não será permitida a utilização de serviços de streaming, tais como Rádios On-Line, Youtube, Google Video e afins.
- Não será permitida a utilização de quaisquer redes sociais (Facebook, Instagram, Twitter) para fins pessoais.
- Não será permitida a utilização de programas de mensagens instantâneas não homologados e autorizados pela Gerência Técnica;
- Não será permitida a utilização de qualquer programa não homologado pela Gerência Técnica que faça acesso à internet;

8 Política de utilização de e-mails

Esta política visa estabelecer responsabilidades e requisitos básicos de uso dos serviços de correio eletrônico, no ambiente de Tecnologia da Informação da JBCRED.

Prover a comunicação é, sem dúvida, a essências das redes. As pessoas procuram se corresponder de maneira mais rápida e fácil possível. O correio eletrônico (e-mail) é uma das aplicações que ilustra esta procura. Entretanto, a funcionalidade de correio eletrônico fornecida pela JBCRED deve ser utilizada no interesse do serviço.

A JBCRED disponibilizará um e-mail para seus colaboradores, a qual deverá ser utilizada exclusivamente para troca de mensagens relacionadas com a atividade desempenhada na instituição.

A JBCRED poderá monitorar a utilização do serviço de e-mail, inclusive analisar o conteúdo das mensagens, de forma a garantir a confidencialidade das informações transitadas.

A JBCRED não se responsabilizará por qualquer mensagem enviada por seus funcionários ou colaboradores que venham a ferir qualquer tipo de legislação vigente, ficando o emissor da mensagem responsabilizado por quaisquer danos causados.

Não será permitida a utilização das contas de e-mail para envio de arquivos não relacionados com a atividade desempenhada, principalmente material fotográfico, vídeos, músicas e apresentações não relacionadas com os objetivos da empresa.

Cada colaborador receberá uma conta cujo nome será gerado pela gerência técnica.

A JBCRED adotará mecanismos para evitar a disseminação de vírus, trojans, códigos maliciosos e demais pragas virtuais no envio ou recepção de e-mail. Esta medida não exime a responsabilidade e os cuidados que o colaborador devem adotar para evitar danos aos recursos disponibilizados e roubo de informações. Algumas mensagens suspeitas poderão ser descartadas sem aviso prévio.

Não será admitido em qualquer hipótese a utilização de e-mails que não sejam do domínio jbcred.com.br ou jbcredsa.com.br. O colaborador da JBCRED deverá respeitar todas as seguintes regras:

- É proibido o assédio ou perturbação de outrem, seja através de linguagem utilizada, frequência ou tamanho das mensagens.
- É proibido o envio de grande quantidade de mensagens de e-mail ("spam") que, de acordo com a capacidade técnica da Rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política.
- É proibido reenviar ou de qualquer forma propagar mensagens em cadeia ou pirâmides, independentemente da vontade do destinatário de receber tais mensagens.
- É proibido o envio de e-mail mal-intencionados ou sobrecarregar um usuário, site ou servidor com e-mail muito extenso ou numerosas partes de e-mail.
- Caso a empresa julgue necessário haverá bloqueios:
  De e-mail com arquivos anexos que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.
  De e-mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.
- É proibido forjar qualquer das informações do cabeçalho do remetente.
- Não é permitido má utilização da linguagem em respostas aos e-mail comerciais, tais como abreviações de palavras.

- É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis.
- É obrigatória a utilização do protocolo IMAP para recebimento dos e-mails provenientes do domínio jbcred.com.br e jbcredsa.com.br.
- É obrigatória a utilização de software homologado pelo departamento técnico, para ser o cliente de e-mail.
- É obrigatória a utilização de assinatura nos e-mails que deverá ser confeccionado pela gerência técnica.
- É terminantemente proibido abrir anexos com as extensões .bat, .exe, .src, .lnk, .vbs, .com, e dll.
- Os usuários de e-mail não devem abrir links contidos na mensagem, principalmente se estes links apontarem para o download de arquivos.
- É proibido enviar e-mails do tipo corrente, aviso de vírus, avisos de grandes empresas, criança desaparecida, criança doente, promoções e etc.
- É proibido utilizar o e-mail para envio de mensagens pessoais.
- É proibido abrir mensagens suspeitas, enviadas por desconhecidos, ou assunto alheio aos interesses da instituição.

9 Política de utilização das estações de trabalho e rede.

Cada estação de trabalho é identificada de forma única na rede, assim como cada colaborador. Desta forma, é possível descobrir quem fez, o que fez e de onde (qual computador) partiu aquele ato. Com isto, torna-se evidente a importância de não deixar o computador com sua senha aberta na sua ausência. Sempre efetue logoff antes de ausentar-se da sua mesa, isto evita que alguém se utilize da sua senha para cometer atos ilícitos que ficarão registrados como sendo seus. Caso se ausente da sua mesa você também pode efetuar o bloqueio da estação para sua maior segurança.

O colaborador deverá observar as seguintes questões de segurança relativas à sua estação de trabalho:

- Não instalar ou remover qualquer tipo de software / hardware sem autorização expressa da Gerência Técnica.
- Não fazer uso de arquivos de música, filmes, fotos ou software protegidos por direitos autorais, nem de qualquer tipo de pirataria.
- Manter na sua estação somente o que for supérfluo ou pessoal. Todos os dados relativos à empresa devem ser mantidos no servidor, onde existe um sistema de backup diário.
- Não manter nos diretórios da rede arquivos pessoais, principalmente fotos, músicas, vídeos e etc., sob pena de exclusão dos mesmos sem prévio aviso.
- Utilização de quaisquer tipos de jogos ou outros aplicativos que possam reduzir o desempenho dos colaboradores.

Os documentos e arquivos relativos à atividade desempenhada pelo funcionário ou colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor de rede, o qual possui rotinas diárias de backup de arquivos.

Não é permitido utilizar os recursos disponíveis como, gravador de CD ou DVD, impressoras e etc., caso existam, para atividades pessoais ou ilegais.

A JBCRED poderá inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas áreas privativas da rede, visando assegurar o rígido cumprimento desta política.

O colaborador da JBCRED deverá zelar pela sua estação de trabalho tomando cuidado principalmente com alimentos e bebidas derramas sobre ela.

Haverá padronização das permissões de acesso a dados para que cada departamento somente tenha acesso ao que lhe diz respeito.

10 Política de trabalho por Acesso Remoto.

O Acesso remoto é uma tecnologia que permite que um computador consiga acessar um servidor privado – normalmente de uma empresa – por meio de um outro computador que não está fisicamente conectado à rede. Esta funcionalidade pode ser habilitada a qualquer momento para que algum colaborador possa fazer algum trabalho específico remotamente. Para que o colaborador tenha este acesso será necessário a aprovação da alta gestão da JBCRED, sendo a princípio negado o acesso remoto a todos os colaboradores inclusive aos de TI. A solicitação deverá ser encaminhada a gerência de TI que junto ao setor de RH conseguirá a liberação do acesso.

Não será permitida a utilização de nenhum programa para esta situação como TeamViewer, AmmyAdmin, AnyDesk, UltraVNC e quaisquer outros com a mesma funcionalidade. Após a liberação da alta gestão o setor de TI encarregará de fornecer este acesso remoto.

11 Política de Realizações de Backup

A JBCRED adotará independentemente do tamanho, procedimentos de cópias de segurança (backup) e recuperação (restore) de informações relevantes ao negócio. Será levado em consideração as seguintes premissas para armazenamento das informações:

- Realização dos backups para diminuir os riscos de continuidade do negócio.
- Manter os backups em local distante da localidade dos dados originais.
- Verificação da integridade das informações armazenadas.
- Avaliação das funcionalidades dos procedimentos de armazenamento.
- Identificação dos procedimentos desatualizados ou ineficazes.
- Identificação falhas ou defeitos.

São de inteira responsabilidade do departamento de Tecnologia da Informação da JBCRED os procedimentos relacionados à política de backup de dados da empresa apresentados a seguir:

- Documentar, testar e avaliar regularmente as tarefas de backup.
- Aplicar testes de recuperação e validação dos backups mensalmente.
- Alocar o servidor de backup em local seguro e isolado, visando a segurança e integridade dos dados.

Os backups serão feitos automáticos e diariamente em períodos que não afetem a atividade da empresa causando lentidão na rede.

Antes do descarte de qualquer mídia física utilizada para o armazenamento das informações da JBCRED, será assegurado de que as informações importantes foram salvas e de que as mídias sejam totalmente destruídas para que a confidencialidade das informações seja mantida.

12 Descumprimento das Regras e Penalidades

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

- Advertência verbal.
- Advertência formal.
- Suspensão por tempo determinado.
- Demissão por justa causa.

Todos os funcionários ao tomarem conhecimento de qualquer incidente de segurança da informação devem informar o ocorrido, imediatamente, à administração do TI pelo e-mail (tecnologia@jbcred.com.br).

13 Considerações Finais

Fica estabelecida a obrigatoriedade, a todos os atuais e novos funcionários e Colaboradores, da assinatura da declaração de conhecimento à Política de Segurança da
JBCRED.

14 Vigência e Validade

A presente política passa a vigorar a partir da data de sua homologação e publicação na Intranet da JBCRED sendo válida por tempo indeterminado e podendo ser revisada e alterada a qualquer momento.

15 Declaração da Política de Segurança

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
JBCRED Sociedade de Crédito Financiamento e Investimento

Declaro estar ciente das normas e procedimentos referentes à Política de Segurança da Informação da JBCRED. Sei que para o bom funcionamento dos processos de trabalho é fundamental a leitura e cumprimento de todas as normas desse documento.

FUNCIONÁRIO: _____

SETOR: _____

ASSINATURA:_____

DATA:_____

16 Comunicação ao Mercado conforme Resolução do BCB nº. 4893/2021.

Em atendimento às orientações da Resolução 4893/2021 do BCB, divulgamos o procedimento padrão de atendimento aos fatos relevantes que podem resultar em paralisação de atividades e contingenciamento das mesmas.

Até o presente momento, não temos contas digitais ou quaisquer outras contas com necessidade de acesso de informações de forma on-line e em real-time, entretanto o assunto é de extrema importância. Desta forma ocorrências destas deverão ser tratadas de maneira a suspender os riscos, detectar a fonte do problema e estabilizar o ambiente produtivo.

Como procedimento, nós deveremos:

- Formalizar aos controladores o fato por correio eletrônico e outras mídias, sempre que ocorrer.
- Formalizar à Auditoria Interna e disponibilizar o material à Auditoria Independente para análise da relevância dos fatos.
- Formalizar ao público através de nota em nossa página principal (website) sempre que ocorrer.
- Formalizar ao BCB o ocorrido e seu desdobramento de forma a cumprir o Art.20º. da Resolução 4893/2021 com o envio do formulário modelo anexo neste material, sempre que ocorrer.
- Estabelecer as linhas de resolução com eventual auxílio de corpo técnico externo (consultores) para mitigar novas ocorrências de fatos relevantes.
- Garantir total transparência a todos os envolvidos direta ou indiretamente no acompanhamento do fato.

Modelo Padrão de Comunicação ao Público – Contingência e Suspensão de Atividades.

JBCRED S/A – Sociedade de Crédito Financiamento e Investimento.

FATO RELEVANTE

A JBCRED S/A SCFI em cumprimento a Resolução 4893*/2021 do BCB/CMN vem informar aos controladores, ao DESUC-BCB e ao Mercado que : (exemplo) sofreu na data de DD/MM/YYYY ataque cibernético identificado por nosso pessoal técnico que resultou em (exemplo) paralisação das atividades regulares a partir do dia DD/MM/YYYY.*

Em razão do ocorrido, a empresa iniciou os procedimentos de investigação e isolou os elementos geradores do fato de forma a garantir a segurança de seu data center, entretanto acarretando suspensão temporária de suas operações.

Como forma contingencial, as operações de:

- Crédito Novos – Ficou suspensa até a regualarização. (exemplo)
- Envio de Lotes aos Parceiros de Cobrança Terceirizada – Ficou suspensa até a regularização (exemplo).
- Pagamentos – Conforme contingência do Departamento Financeiro.

A JBCRED S/A está empreendendo todos os seus esforços para investigar as circunstâncias do ataque, avaliar se existem impactos sobre seus negócios e terceiros, e determinar as medidas a serem tomadas. A Companhia manterá o mercado informado dos desdobramentos deste evento.

São Paulo, DD de MMMMMM de YYYYY

Em necessidade de contato:

Nome do Diretor Responsável por TI , Departamento, Telefone, E-mail.
Nome do Gerente de TI , Telefone, E-mail.
Nome do Diretor do Departamento Comercial e Financeiro, Telefone, Email.