POSEC

Políticas de Segurança Cibernética

VERSÃO PÚBLICA exigida pelo BACEN

Resolução CMN nº 4.658 de 26/4/2018

SBcrédito

1. OBJETIVOS

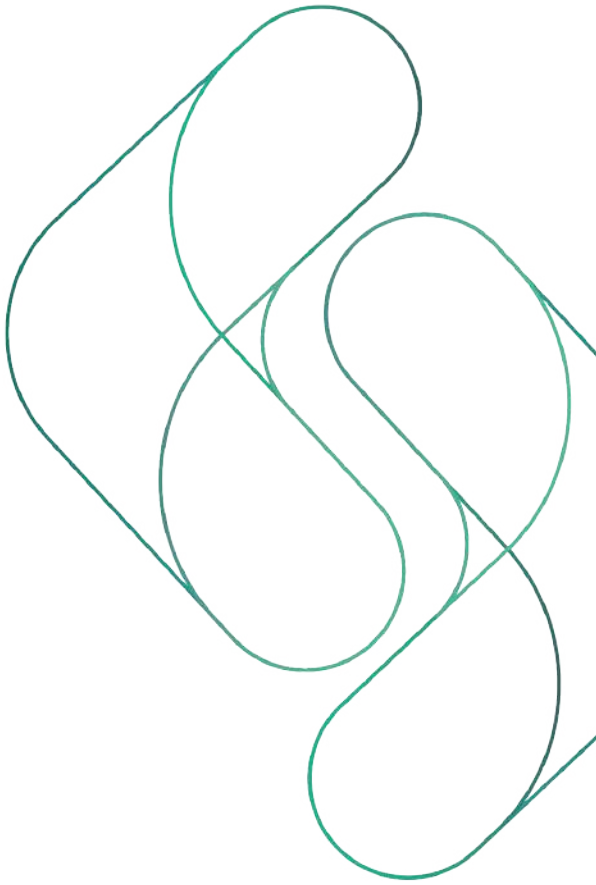
A Política de Segurança Cibernética (POSEC) da SB Crédito objetiva garantir a integridade, a disponibilidade e a divulgação dos dados e sistemas de informação utilizados pelo nosso modelo. A POSEC busca também assegurar a aplicação dos princípios e diretrizes de segurança da informação, incentiva o compartilhamento de informações e a transparência com devido cuidado às restrições e procedimentos internos, propaga a conscientização dos controles adotados para reduzir a vulnerabilidade da SB Crédito a incidentes cibernéticos e a redução do risco de vazamento de informações, além de controles específicos, voltados à rastreabilidade da informação, que vise a segurança de informações sensíveis, a classificação de dados e responsabilização por vazamento, o registro e a análise da causa e do impacto.

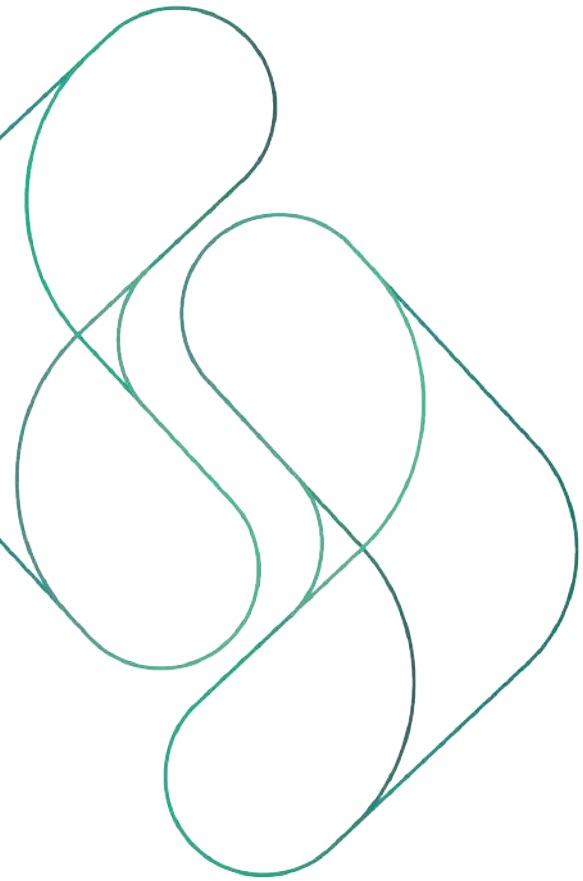
1.1 Abrangência

A POSEC aplica-se a todos os colaboradores, clientes, parceiros de negócio e prestadores de serviços ou terceiros da SB Crédito. Entende-se como “colaboradores” todos os empregados, administradores, estagiários e menores aprendizes da SB Crédito.

1.1.1 Segurança de Sistemas e Tecnologia da Informação

A SB Crédito faz uso de sistemas e soluções tecnológicas, bem conhecidos pelo mercado, por suas características e funcionalidades avançadas de infraestrutura com compromisso sólido em reduzir a vulnerabilidade a incidentes e assim proporcionar maior segurança cibernética para seus clientes e usuários. Utilizamos antivírus, firewall de proteção da rede contra-ataques, sistema operacional e navegadores atualizados.





Na SB Crédito todos os dispositivos internamente utilizados são atualizados pela equipe de TI antes de serem disponibilizadas para seus colaboradores. Dessa maneira, assegurando que os sistemas operacionais, navegadores e demais sistemas de informação atendam padrões internacionais de segurança da informação e realizem todas as atualizações críticas em tempo hábil.

1.2 DEFINIÇÕES, SIGLAS E ABREVIATURAS

Para os fins desta Política de Segurança Cibernética (POSEC) consideram-se as definições das siglas, abreviaturas e expressões que constam no Capítulo 13 - Glossário de Definições.

1.3 Princípios

São princípios da Política de Segurança Cibernética:

a) Todos os dados e informações usados na SB Crédito são considerados um ativo de informação particular da empresa e devem ser tratados com discrição adequada;

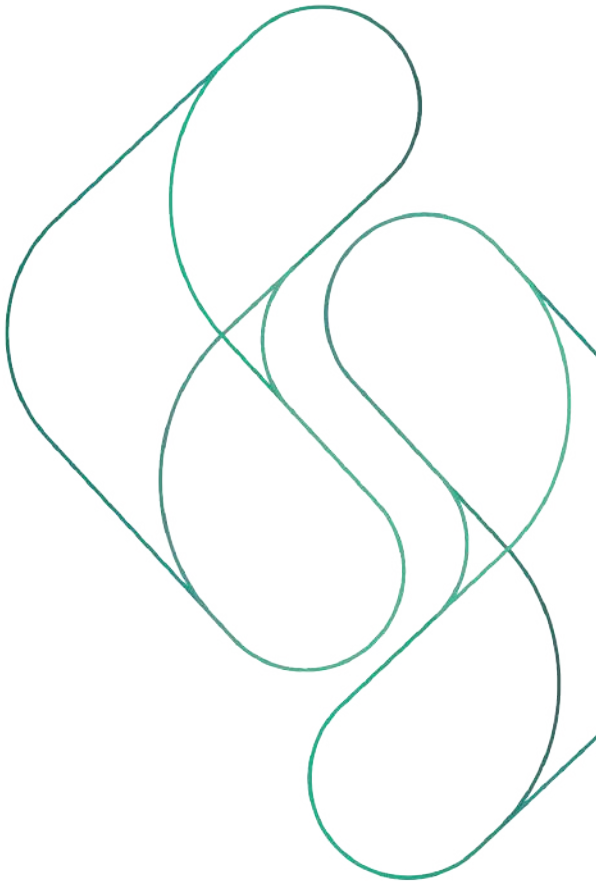
b) Todos os colaboradores da SB Crédito conhecem e acatam a POSEC;

c) A SB Crédito divulga, conscientiza e mantém programa de treinamento sobre Segurança Cibernética;

d) A SB Crédito mantém um Comitê de Segurança da Informação;

e) A SB Crédito gerencia os softwares utilizados pela organização e;

f) A SB Crédito procura prover todos os recursos necessários para garantir a segurança cibernética.



2. ACORDOS DE CONFIDENCIALIDADE

Com intuito de assegurar a confidencialidade, integridade e disponibilidade dos dados, a SB Crédito determina que todos os novos colaboradores; parceiros de negócio e prestadores de serviços ou terceiros devem tomar conhecimento prévio das nossas políticas de cibersegurança e políticas de conduta ética. Considera-se como “colaboradores” todos os empregados, administradores, estagiários e menores aprendizes da SB Crédito.

Todo evento ou incidente de segurança da informação ocorrido na SB Crédito deve ser registrado em e-mail e reportado para seguranca@sbcredito.com.br para tratamento e monitoramento até a resolução. Sendo que os responsáveis de TI farão a classificação do incidente quanto a urgência, impacto e prioridade.

3. POLÍTICAS DE USO DE INTERNET

3.1 Objetivo

Esta política objetiva estabelecer regras gerais, definir responsabilidades e requisitos básicos de utilização da Internet na rede SB Crédito visando assegurar a segurança cibernética.

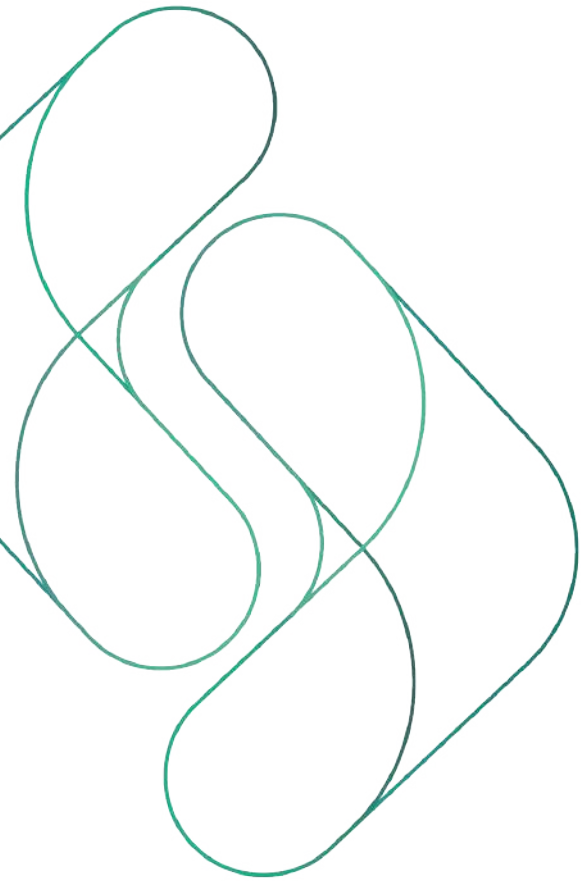
3.2 Abrangência

Esta política se aplica a todos os colaboradores, prestadores de serviços, terceirizados, estagiários, fornecedores ou quaisquer outros indivíduos ou entidades que venham a ter acesso e/ou utilizar, direta ou indiretamente, as informações ou os ativos de informação de toda rede SB Crédito.

3.3 Determinações Gerais

Todo o acesso à internet no ambiente corporativo da SB Crédito será feito exclusivamente pelos meios autorizados e configurados pelo departamento de TI.

3.3.1 O acesso à internet é disponibilizado pela SB Crédito para uso nas atividades relacionadas ao trabalho, sendo o uso para fins pessoais limitado aos princípios da ética, razoabilidade e legalidade. A possibilidade de acesso a qualquer serviço da internet não implica em autorização para sua utilização.



3.3.2 Os prestadores de serviços e terceirizados devem seguir os procedimentos para acesso à internet que são executados conforme norma operacional de registro de usuários e permissionamento de serviços;

3.3.3 Para ter acesso à internet, o usuário deve receber orientações quanto ao uso correto desse recurso para assegurar que todos estão cientes das implicações referentes à segurança cibernética.

3.3.4 Os conteúdos da internet, utilizados no exercício das atividades da SB Crédito, devem ser referenciados de forma a identificar claramente sua origem de modo a respeitar o direito autoral, proibindo-se a cópia, reprodução ou distribuição sem prévia autorização.

3.3.5 A cada usuário cabe o acatamento das seguintes práticas:

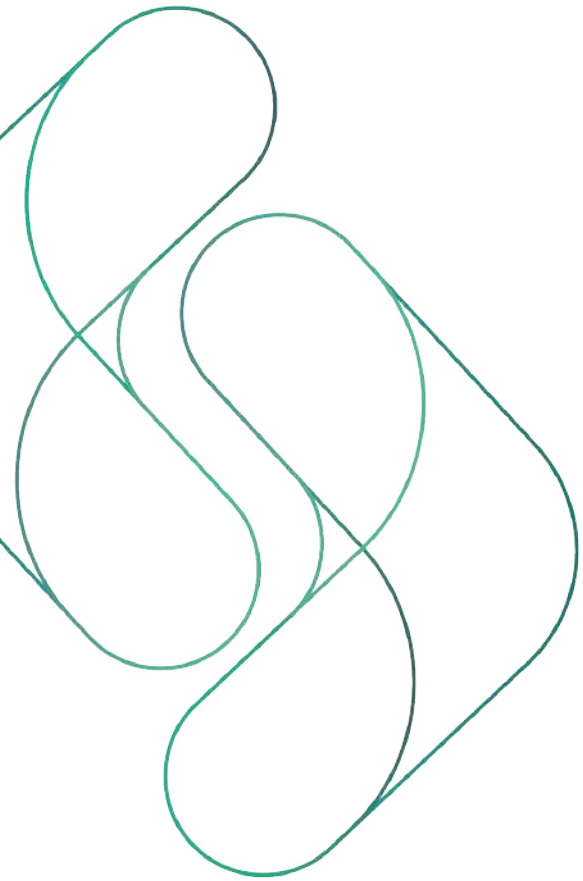
a) Não utilizar do acesso à internet para comprometer a segurança (integridade, confidencialidade ou disponibilidade) de computadores, sistemas ou serviços de instituições privadas ou governamentais;

b) Não permitir que outros usuários façam uso da Internet com suas credenciais. O acesso concedido ao usuário é pessoal e intransferível;

c) Certificar-se de que dados ou informações pessoais e sigilosas sejam transmitidas de forma segura, por meio de uma conexão segura, normalmente identificada com a denominação HTTPS:// na barra de endereço e o símbolo de um cadeado;

d) Desconectar-se com segurança de sistemas web, utilizando links específicos para este fim, como “Sair”, “Log off” ou “Desconectar”. Evitar simplesmente fechar o navegador, pois isso mantêm a conexão ativa por alguns minutos, possibilitando a sua utilização por um usuário mal-intencionado e

e) Não utilizar o recurso de “salvar” ou “lembrar” senhas, disponíveis em muitos navegadores de Internet.



3.3.6 Fica liberado o acesso a sítios de governo, de órgãos de ensino e pesquisa, de organismos internacionais de pesquisa, de órgãos técnico-normativos e a jornais e revistas de cunho cultural e educativo, bem como a outros de interesse institucional.

3.3.7 Os usuários da rede devem reportar os incidentes que afetem a segurança dos ativos ou o descumprimento da Política de Segurança Cibernética à Gerencia de TI.

4. CRITÉRIOS DE CLASSIFICAÇÃO DOS DADOS

A classificação dos dados consiste na definição de níveis de proteção que cada dado deve receber. Tal classificação serve para garantir que nenhum dado seja divulgado indevidamente e que apenas as pessoas que precisem desses dados recebam acesso aos mesmos. A classificação dos dados faz parte das exigências da ISO 27001 e LGPD.

Os dados confidenciais devem ser protegidos por criptografia e requerem sigilo absoluto. As informações utilizadas no dia a dia operacional da SB Crédito recebem a classificação conforme a finalidade, sensibilidade e acesso. Os dados são classificados como: confidenciais, restritos, de uso interno ou públicos.

4.1 Confidencial: É o nível mais alto de segurança. Os dados confidenciais são aqueles que, se divulgados interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou denegrir à imagem da empresa e sua marca, podendo também causar a perda de clientes, afetar a competitividade e crescimento das operações. São protegidos por criptografia.

4.2 Restrito: É o nível médio de segurança. São dados estratégicos que devem estar disponíveis apenas para grupos restritos de colaboradores. A exemplo, essas informações podem ser protegidas restringindo o acesso à uma pasta ou diretório da rede.

4.3 Interno: Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

4.4 Público: São dados que não necessitam de proteção contra vazamentos, pois podem ser de conhecimento público. No entanto, cabe ressaltar dois pilares: a integridade e disponibilidade.

5. CORREIO ELETRÔNICO E COMUNICAÇÕES DIGITAIS

5.1 Introdução

Esta política objetiva prover diretrizes e restrições para o uso prudente do correio eletrônico e canais de comunicação digitais da SB Crédito com bases nos requisitos de cibersegurança. Esta política operacional aplica-se à todos os empregados, colaboradores, prestadores de serviços, terceirizados, fornecedores ou quaisquer outros indivíduos ou entidades que venham a ter acesso e/ou utilizar, direta ou indiretamente, as informações ou os ativos de informação da rede SB Crédito.

5.2 Correio Eletrônico

A conta de correio eletrônico pertence a SB Crédito e é fornecida para realização das atividades correlatas a cada colaborador, de forma ágil, promovendo a comunicação eficiente e maior fluidez dos dados e informações para a tomada de decisão eficaz. Qualquer serviço digital que seja criado com a conta de e-mail da SB Crédito deve seguir os mesmos princípios de conduta ética e ser utilizado para aprimorar a realização de atividades da SB Crédito. O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível.

5.3 Responsabilidade do usuário:

São de responsabilidade do usuário:

a) A proteção do sigilo de sua senha de acesso a fim de evitar a utilização da conta de correio eletrônico por outrem, cabendo a responsabilização civil e/ou criminal do mesmo pelos danos cometidos através da má utilização do recurso;

b) Os anexos, links, e conteúdo de mensagens enviadas, sob sua identificação;

c) O cuidado quanto a origem dos links e mensagens recebidas a fim de evitar danos;

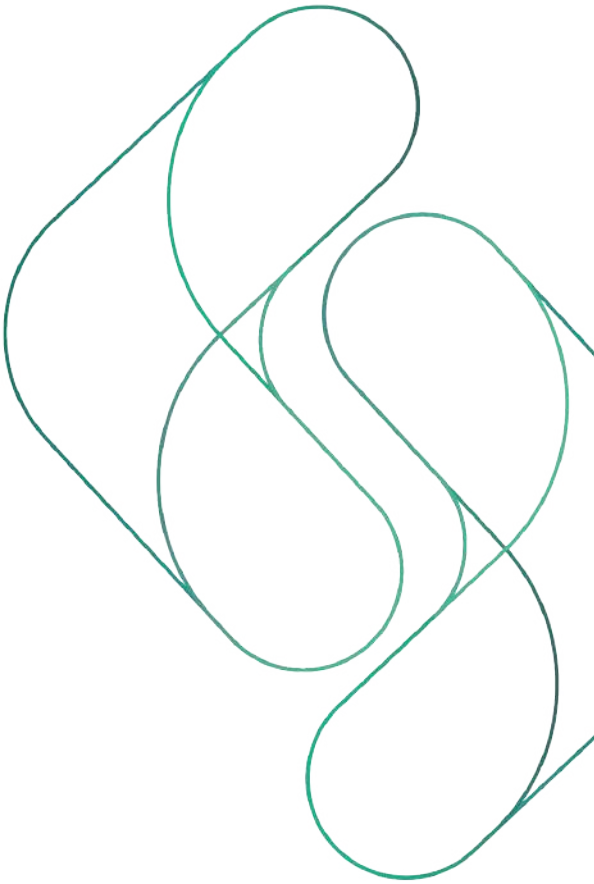
d) A utilização do serviço de correio eletrônico fornecido pela SB Crédito para assuntos exclusivos da instituição;

e) A comunicação à Diretoria de Segurança da Informação (seguranca@sbcredito.com.br) sobre qualquer ocorrência estranha a utilização institucional do correio eletrônico, ocorrida em seu e-mail, ou em sua área de trabalho.

6. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

6.1 Teste de Continuidade de Negócios

A SB Crédito tem a incumbência de manter a continuidade dos negócios em caso de incidente crítico. A SB Crédito tem redundância em seus serviços para continuar operando mesmo com a queda de um ou mais servidores de sistemas. No caso em que um incidente venha a interromper a operação normal, entra em ação o Plano de Continuidade de Negócios. O plano possui o objetivo de identificar os riscos que possam comprometer a continuidade de suas atividades, avaliar o impacto e providenciar a resiliência da SB Crédito, atribuindo a empresa a capacidade de prevenir ou reagir de forma eficiente a estes eventos.



6.2 Prestadores de Serviços de Tecnologia

Os procedimentos e controles voltados à prevenção e ao tratamento de incidentes em relação aos prestadores de serviço de tecnologia são previamente definidos em contratos. Na ocasião de um incidente, o fornecedor do serviço é acionado pela área correlata e é realizado o acompanhamento até resolução final, dentro do período pré-contratado.

Todo prestador de serviços da SB Crédito tem conhecimento da política segurança cibernética e assina um termo de responsabilidade e confidencialidade no uso das informações fornecidas pela SB Crédito estritamente para realização de suas atividades contratadas. Em caso de qualquer incidente, o gestor direto do terceiro é responsável por registrar o caso em e-mail e encaminhar para o departamento de TI com cópia para a direção de Operações e área de RH.

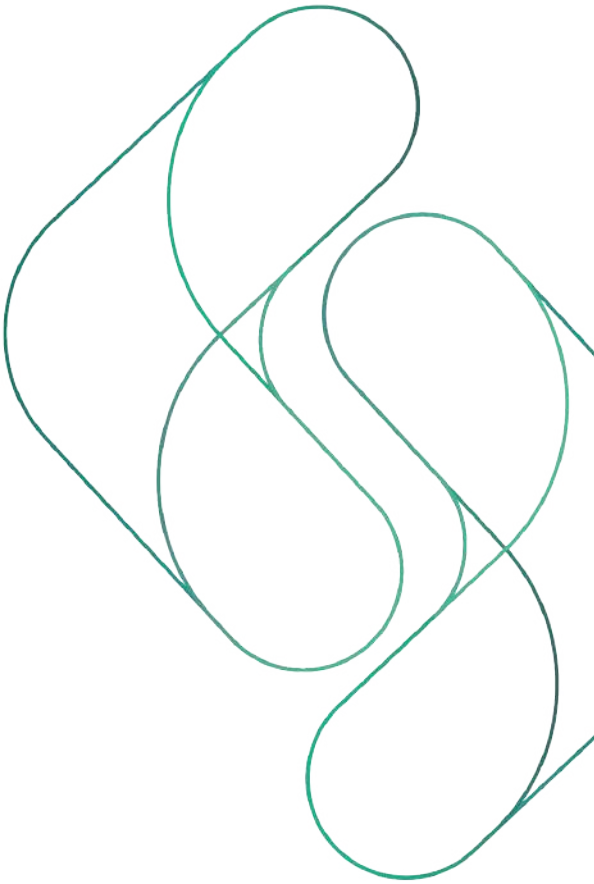
Após o incidente ser recebido, será classificado conforme o impacto nos negócios e o tempo mínimo necessário de resposta (crítico, emergencial ou evento inesperado) e será atribuído um responsável para dar seguimento até resolução final.

6.3 Classificação d criticidade dos Incidentes

Os incidentes relacionados à Segurança Cibernética podem seguir os fatores de criticidade, considerando 03 tipos de situação: Crítica, de emergência e evento inesperado.

6.4 Plano de ação de resposta a incidentes

A SB Crédito dispõe de mecanismos de detecção a intrusão, firewall de rede e equipe de suporte a segurança da informação. Na ocorrência de incidente de segurança, o mesmo deve ser analisado e, após análise, é elaborado um plano de ação para corrigir e/ou melhorar o ambiente e/ou processo com o objetivo de evitar ou minimizar a possibilidade de nova ocorrência. A elaboração e acompanhamento do plano de ação são coordenados pela Área de Tecnologia da Informação com participação das áreas envolvidas no incidente.



6.5 Política de uso de computação de nuvem

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as normativas na resolução 4893 do BACEN, art. 11 até art. 18.

6.6 Política de Custódia de dados para o BACEN

Devem ficar à disposição do Banco Central do Brasil pelo prazo de 05 (cinco) anos:

a) A presente Política;

b) Ata do Conselho de Administração com a aprovação da Política;

c) Documento relativo ao plano de ação e de resposta a incidentes;

d) Relatório anual;

e) Documentação sobre os procedimentos;

f) Documentação que trata no caso de serviços prestados no exterior;

g) Os contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem e

h) Os dados, os registros e as informações relativas aos mecanismos de acompanhamento de controle que visam assegurar a implementação e a efetividade da política se segurança cibernética.

7. POLÍTICA DE ACESSO AOS SISTEMAS DA REDE SB CRÉDITO

Cada indivíduo, na qualidade de colaborador ou prestador de serviços da SB Crédito, é inteiramente responsável pela proteção e utilização de suas senhas e permissões de acesso a sistemas, assim como pelas ações decorrentes da utilização destes acessos.

O acesso e o uso de todos os sistemas de informação, bancos de dados, diretórios da rede e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados.

7.1 Regra de mínimo acesso

A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função. Periodicamente, os acessos concedidos devem ser revistos pela gerência imediata e pelo comitê gestor da segurança da informação.

7.2 Política de Autenticação e Senha

Os usuários da SB Crédito devem:

a) Manter a confidencialidade, memorizar e não registrar a senha. Ou seja, não contar a ninguém e não anotar em papel;

b) Alterar a senha sempre que existir qualquer suspeita do comprometimento e avisar seu gestor imediato com copia de e-mail para o time de segurança cibernética.

c) Selecionar senhas de qualidade, que sejam de difícil adivinhação. Utilizar senhas com letras maiúsculas e minúsculas, números e caracteres especiais com no mínimo 10 dígitos;

d) Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ “logado” com a sua identificação SB Crédito;

e) Bloquear sempre o equipamento ao sair de perto dele. ex.: (Ctrl + Alt + Del ou Win + L)

8. LEIS E REGULAMENTOS

Cabe a todos os prestadores de serviços e parceiros da SB Crédito, conhecer a legislação e cumprir os requisitos legais, normas e padrões locais vigentes.

9. SITUAÇÕES DE EXCEÇÃO

A SB Crédito está preparada para trabalhar em situações de exceção e manter o atendimento online disponível para seus clientes de forma confiável e escalável. Os principais servidores de sistemas da SB Crédito possuem redundância em localidades afastadas e distintas, o que permite assegurar que mesmo em situação de incidente grave, os serviços fornecidos permanecerão disponíveis para os clientes.

10. SEGURANÇA DE USO DE RECURSOS DE INFORMAÇÃO

Os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos devem ser acompanhados pós a sua cópia, impressão ou utilização e devem ter seu descarte realizado de forma adequada. Apenas os equipamentos e softwares autorizados pela SB Crédito podem ser instalados e conectados à rede da SB.

10.1 Treinamento de segurança

O conhecimento de segurança da informação é difundido internamente através de programas de capacitação ministrados para todos os colaboradores, certificando dessa maneira que todos tenham ciência das possíveis ameaças e vulnerabilidades que envolvem a segurança cibernética, bem como quais são os procedimentos a serem seguidos em situações de crise ou incidentes.

A SB Crédito incentiva e promove uma cultura de segurança dentro da instituição, visando proteger os objetivos citados nesta política, e principalmente proteger a informação. A SB Crédito tem consciência que as atividades de segurança cibernética, estão em constante evolução. Sendo assim, os procedimentos e controles relacionados com o tema, serão revistos com periodicidade, promovendo uma melhoria contínua do ambiente de segurança cibernética.

10.2 Compartilhamento de informações

A SB Crédito, em seu compromisso com a segurança cibernética e transparência, compartilha com o BACEN todos os registros, as análises da causa e dos impactos, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, tempestivamente, sempre que solicitado.

10.3 Relatório anual

De acordo com a Resolução 4.893 do BACEN, anualmente, até o 31 de março, a SB Crédito deverá emitir um relatório sobre a implementação do plano de ação de respostas a incidentes, com data base de 31 de dezembro do ano anterior ao relatório, contendo:

a) A efetividade da implementação das ações a serem desenvolvidas pela instituição para adequar suas estruturas aos princípios e às diretrizes da política de Segurança Cibernética;

b) O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

c) Os incidentes relevantes ocorridos no período e

d) Resultado dos testes de continuidade de negócios.

11. ATUALIZAÇÃO E VIGÊNCIA

A POSEC tem vigência mínima anual, mas pode ser alterada para refletir modificações da regulamentação ou legislação vigente e aplicar aprimoramentos resultantes dos processos de melhoria contínua internos da SB Crédito. A versão final desta política deve ser publicada no portal da SB de forma pública.

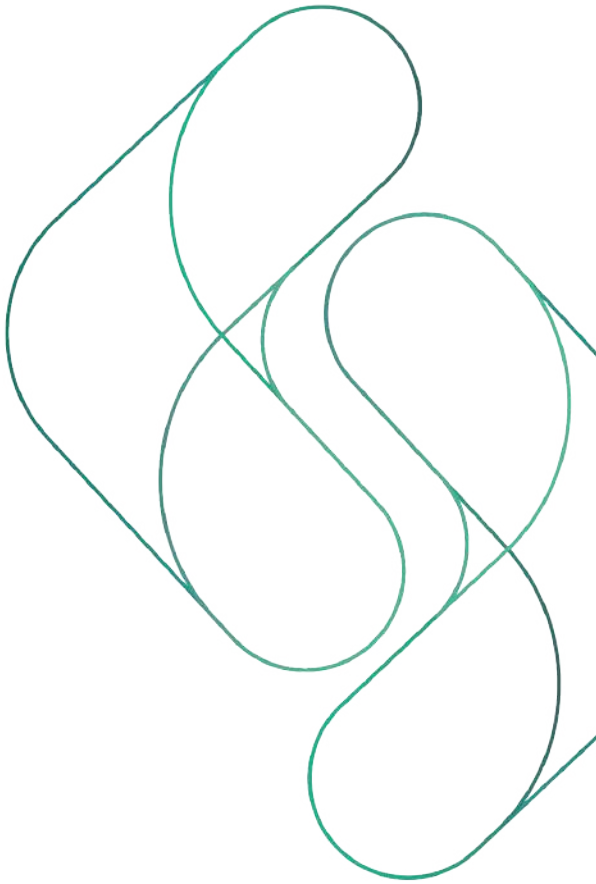
12. POLÍTICA DE USO DE DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

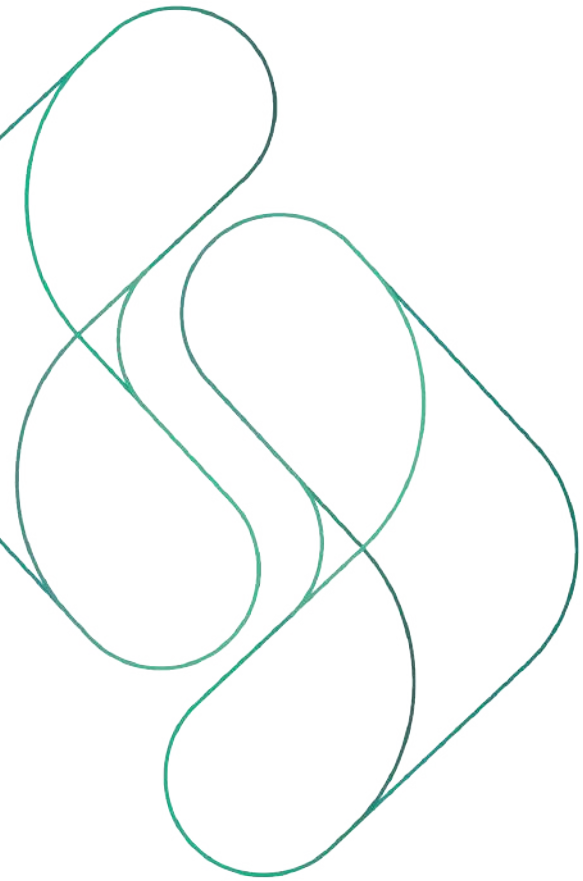
12.1 Objetivo

O objetivo da política de uso de dispositivos móveis e trabalho remoto é garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis. Os riscos decorrentes de tal uso devem estar mapeados e gerenciados adequadamente.

12.2 Diretrizes para implementação

Quando dispositivos móveis são utilizados, cuidados especiais devem ser tomados para assegurar que as informações confidenciais e restritas do negócio não sejam comprometidas. A política de dispositivos móveis leva em consideração os riscos de se trabalhar com esses dispositivos móveis em ambientes desprotegidos.





12.3 Transporte de dispositivos móveis

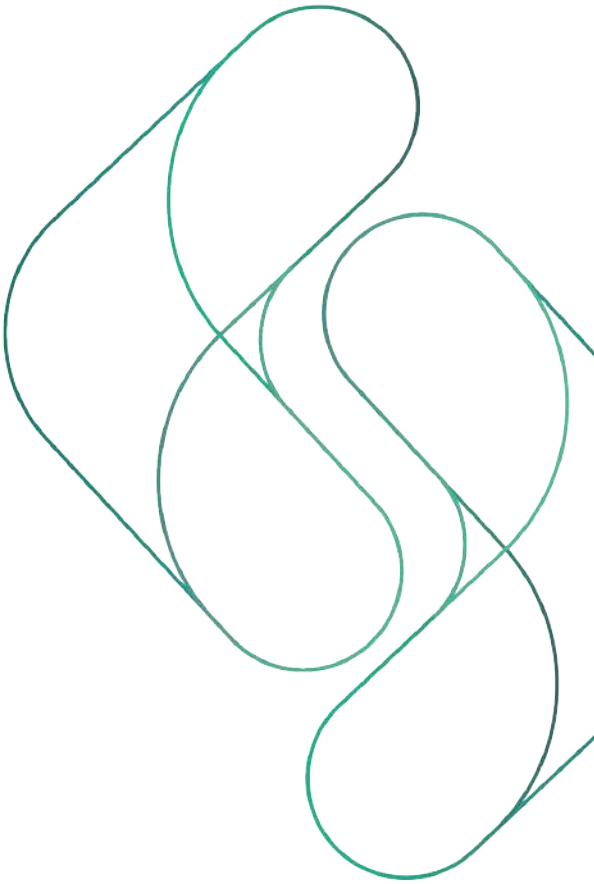
Cuidados devem ser tomados ao utilizar dispositivos móveis (notebooks, tablets, celulares e etc.) em locais públicos, salas de reuniões e outras áreas desprotegidas. Convém que seja estabelecida uma proteção para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nesses dispositivos, por exemplo, através da utilização de técnicas de criptografia e do uso de informação de autenticação secreta.

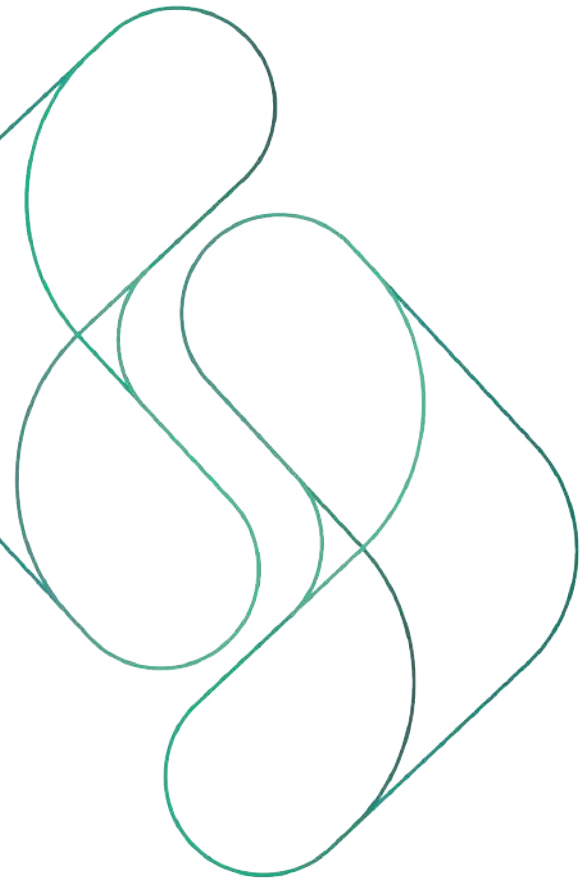
Os dispositivos móveis devem ser protegidos fisicamente contra roubo, especialmente quando deixados, por exemplo, em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião.

Dispositivos móveis que contêm informações importantes, sensíveis e/ou críticas para o negócio, não devem ser deixados sem observação e, quando possível, fisicamente trancados com o uso de travas especiais, ou em um ambiente de acesso físico controlado.

O transporte de dispositivos móveis, tais como notebooks e outros acessórios que possam atrair furtos ou roubo, deve ser feito de preferência no porta-malas dos veículos, seja veículo próprio ou serviço de transporte contratado por aplicativo, por exemplo.

Um treinamento ou divulgação deve ser programado para as pessoas que usam dispositivos móveis, como forma de aumentar a conscientização quanto aos riscos adicionais decorrentes desta forma de trabalho, e os controles que se recomenda implementar.





12.4 Recomendações adicionais

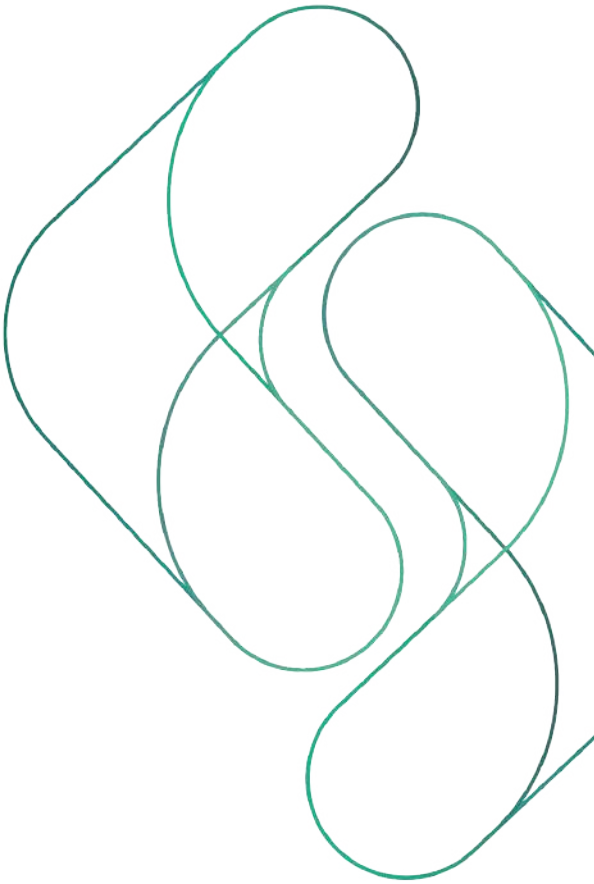
Conexões de dispositivos móveis sem fio são similares a outros tipos de conexões de rede, mas possuem diferenças importantes.

a) Alguns protocolos de segurança sem fio são imaturos e possuem vulnerabilidades conhecidas. Recomenda-se não se conectar a redes que utilizam protocolo WEP ou WPS, seja no uso doméstico ou em outras redes, tais como coworkings, hotéis, eventos, cafés, etc. ;

b) Informações armazenadas em dispositivos móveis podem não ser passíveis de cópia de segurança por conta de limitações da largura de banda da rede ou porque dispositivos móveis podem não estar conectados no momento em que a cópia de segurança for agendada. Nesses casos, é recomendado que o usuário verifique manualmente se o backup foi realizado para reter o risco perdas.

12.5 Trabalho Remoto

A SB Crédito permite a execução de atividades de trabalho remoto. As informações de negócio acessadas, processadas ou armazenadas em locais de trabalho remoto devem também ser protegidas seguindo as restrições da Política de Segurança Cibernética. Deve ser utilizado VPN para acessar os serviços remotos e o dispositivo remoto deve apresentar sistemas de segurança atualizado, tais como antivirus, firewall e sistema operacional (MS Windows ou Linux).



13. GLOSSÁRIO DE DEFINIÇÕES:

AD - ACTIVE DIRECTORY:

Ferramenta de gerenciamento de usuários de rede, bastante utilizada para autenticar um usuário e é denominada serviço de diretório. Todo computador que faz parte do domínio (Grupo da empresa), seja uma estação de trabalho, servidor ou impressora, deve ter uma conta no Active Directory.

AMEAÇA:

Causa potencial de um incidente que pode resultar em dano para o negócio. Qualquer objeto ou circunstância que viabilize a exploração de uma vulnerabilidade. Qualquer causa potencial de um incidente pode ser considerada como sendo uma ameaça. Estas ameaças podem ser acidentais ou deliberadas.

ANÁLISE DE VULNERABILIDADE DE CÓDIGO:

Teste de software que verifica a lógica interna do sistema em busca de falhas, inconformidades e vulnerabilidades, apontando a linha de código que causa o erro e que precisa ser corrigida. Também conhecido como teste estrutural ou de caixa-branca;

ANÁLISE DE VULNERABILIDADE DE APLICAÇÃO:

Teste de software que verifica o comportamento externo da aplicação em execução para identificar anomalias ou vulnerabilidades, sendo capaz de simular ataques à aplicação e mostrar os efeitos de uma exploração. Também conhecido como teste funcional ou de caixa-preta;

BACKUP:

É um termo inglês que tem o significado de cópia de segurança. É frequentemente utilizado em informática para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.

COLABORADOR:

Qualquer pessoa que seja membro do Conselho de Administração, Diretor Executivo, funcionário, estagiário, prestador de serviços ou mandatário, a título permanente ou ocasional, da SB Crédito.

CONFIDENCIAL:

É o nível mais alto de segurança. Os dados confidenciais são aqueles que, se divulgados interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da empresa. Devem ser protegidos por criptografia.

DOWNLOAD:

Constitui o ato de copiar um arquivo da rede (internet). O arquivo (download) pode ser copiado por e-mail, WhatsApp, Discord, chat, Telegram, website etc. Consiste na cópia de dados da internet. Quando recebemos um novo e-mail, fizemos um download.

HACKER:

É um termo inglês para definir um invasor ou um grupo de invasores que buscam atacar seu dispositivo pessoal ou de empresas, tais como computadores, celulares, servidores, roteadores etc.

INCIDENTE DE SEGURANÇA DE INFORMAÇÃO:

Qualquer evento que afete ou possa afetar a integridade, disponibilidade, privacidade, confidencialidade, autenticidade, auditabilidade e/ou confiabilidade da informação ou sistemas de informação da SB Crédito, incluindo qualquer ação ou omissão, deliberada ou não, que viole a regulação vigente pertinente a segurança de informação.

INFORMAÇÃO:

Todos os dados e registros, tangíveis ou intangíveis, incluindo voz e imagem, independentemente do seu formato, modo de tratamento, meio de transmissão - físico ou lógico - relativos à vida da instituição SB Crédito.

INTERNO:

Representa baixo nível de confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação. Links: a hiperligação, ou simplesmente uma ligação (em inglês, hyperlink e link), é uma referência dentro de um documento em hipertexto a outras partes desse documento ou a outro documento. Muito utilizado para repassar um website para outra pessoa.

MEDIA ACCESS CONTROL (ENDEREÇO MAC):

Termo relacionado a redes de computadores. Basicamente é um endereço físico e único que conecta um dispositivo à rede.

POSEC:

Política de Segurança Cibernética SB Crédito.

PÚBLICO:

São dados que não necessitam de proteção contra vazamentos, pois podem ser de conhecimento público. No entanto, cabe ressaltar dois pilares: a integridade e disponibilidade.

REQUISITOS DE SEGURANÇA:

Conjunto de necessidades de segurança às quais o software deve atender compreendendo aspectos funcionais e não funcionais;

RESTRITO:

É o nível médio de segurança. São dados estratégicos que devem estar disponíveis apenas para grupos restritos de colaboradores. A exemplo, essas informações podem ser protegidas restringindo o acesso à uma pasta ou diretório da rede.

RISCO:

Potencial exploração de uma vulnerabilidade como caminho para a concretização de uma ameaça, com a perspectiva de impactos negativos;

SEGURANÇA DA INFORMAÇÃO:

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

SISTEMA:

Coleção de componentes organizados para desempenhar uma determinada função ou conjunto de funções. Um sistema pode ser digital ou não. O desenvolvimento e manutenção de um sistema de computador ocorre ao longo do seu ciclo de vida.

SSL - SECURE SOCKET LAYERS:

Padrão de segurança que cria um canal criptografado entre um servidor web e um navegador.

TRILHAS DE AUDITORIA:

Em segurança cibernética é um histórico de ações realizadas no sistema, também conhecido como 'log' do sistema. A Trilha é um alvo clássico em ataques cibernéticos, onde o invasor busca apagar ou alterar o rastro de seu ataque.

UPLOAD:

Consiste na cópia de dados para internet. Quando enviamos um e-mail, fazemos um updload.

VPN:

Virtual Private Network

VULNERABILIDADE:

Ponto fraco de procedimento, arquitetura, implementação ou controles internos de um sistema que pode ser acidentalmente ou intencionalmente explorado.

TIPOS DE ATAQUES VIRTUAL:

ENGENHARIA SOCIAL:

Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto desta política, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido “171” ou “conto do vigário” utiliza engenharia social.

MAIL BOMBING:

Envio de mensagens eletrônicas em massa para um determinado destinatário com o objetivo de sobrecarregar o serviço de e-mail e torná-lo inutilizável ou indisponível. Nesse tipo de ataque, são enviados milhares de e-mails simultaneamente originados de fontes diversas.

MALWARE:

Do inglês Malicious software. Conhecido também como Código Malicioso ou software malicioso. Phishing: Nome estrangeiro dado ao ataque virtual em que um farsante se apresenta como uma empresa ou instituição conhecida e de renome com o objetivo

de coletar informações sensíveis, como: dados pessoais, número de cartão de crédito, senhas, entre outros. Esse tipo de ataque faz uso de manipulações psicológicas e seu êxito depende de falhas humanas (ao invés de falhas técnicas), o phishing é classificado como um ataque de engenharia social.

PROXY OU EMULADORES DE PROXY:

São ferramentas que burlam a segurança de rede e podem expor a rede corporativa a ataques e perdas de informações.

RAMSOWARE:

É um software nocivo que é usado para bloquear dados de computadores e servidores através do uso de algum tipo de criptografia. Esse malware é usado por hackers para exigir resgates, para que os dados sejam novamente liberados.

SPAM:

É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Trojan: Em computação, um cavalo de Troia (do inglês, 'Trojan horse', ou, simplesmente, trojan) é qualquer aplicativo mal intencionado que engana os usuários sobre sua verdadeira intenção. O termo é derivado da história grega antiga do cavalo de Troia enganoso que levou à queda da cidade de Troia Vírus de computador: Em informática, um vírus de computador é um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

WEP:

Significa Wired Equivalent Privacy, e é um tipo de chave de segurança. Foi introduzido na tentativa de dar segurança durante o processo de autenticação, proteção e confiabilidade na comunicação entre os dispositivos sem fio. A chave de segurança é um protocolo que criptografa os dados transmitidos por Wi-Fi. Ela também é chamada de chave de criptografia ou chave WEP.

WI-FI OU WIRELESS:

Significa rede sem fio. Popularmente usada para conectar na internet ou intranet de casa ou da empresa.

WPS:

Wi-Fi Protected Setup: é um padrão de segurança de rede que permite que os usuários mantenham facilmente uma rede sem fio doméstica segura.