ESTADO DE GOIÁS
AGENCIA DE FOMENTO DE GOIAS - GOIASFOMENTO

POLÍTICA DE SEGURANÇA CIBERNÉTICA

- Aprovada pelo Conselho de Administração em reunião do dia 14/06/2023 -

PRESIDENTE
Eurípedes José do Carmo

DIRETOR ADMINISTRATIVO E FINANCEIRO
Lucas Fernandes de Andrade

DIRETOR DE OPERAÇÕES
Leandra Adriano de Assis

GERENTE DE TI
Luiz Carlos dos Santos Sardinha

GERENTE DE RISCO
Porthos Ribeiro de Albuquerque Motta

EQUIPE RESPONSÁVEL
Carla Moema Moreira Duarte
Eduardo Tomazett Martins
Frederico Carlos Wilhelms

1. OBJETIVO E ESCOPO:

A Política de Segurança Cibernética da GoiásFomento, que é revisada periodicamente, promove a implantação de medidas preventivas, detectivas e corretivas voltadas ao controle do ambiente cibernético, mitigação de potenciais incidentes de segurança cibernética e redução de vulnerabilidades.

Os objetivos principais de referida Política são:

1) Garantir a confidencialidade, integridade e disponibilidade das informações dos clientes, empregados e fornecedores;

2) Proteger adequadamente os sistemas e informações;

3) Garantir a continuidade dos negócios, protegendo os processos críticos de interrupções;

4) Garantir que sejam respeitadas as finalidades aprovadas durante a prestação de serviços de terceiros quando da contratação de serviços de processamento e/ou armazenamento de dados.

2. ABRANGÊNCIA:

· Unidade Gestora: GETEC.

· Unidade Responsável: Todos os departamentos da GoiásFomento.

· Público-Alvo: Colaboradores, Prestadores de Serviço e Clientes.

· Classificação: Público.

3. AMPARO LEGAL:

Desde a primeira Resolução de 26 de abril de 2018, o BACEN estabelece os critérios a serem cumpridos e obriga as instituições financeiras a adotar segurança cibernética, permitindo que as instituições reguladas avancem de maneira mais organizada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

4. PERIODICIDADE:

Conforme Art. 10 da resolução CMN nº 4.893/2021 a política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente.

5. DEFINIÇÃO:

O uso do termo "empresa" está em reverência à seguinte organização: Agência de Fomento de Goiás S.A.

6. INTRODUÇÃO:

Esta Política de Segurança Cibernética se trata de um conjunto formal de regras pelas quais os stakeholders que possuem acesso à tecnologia da empresa e aos ativos de tecnologia da informação devem obedecer.

Em conformidade com a Resolução CMN nº 4.879, de 26 de fevereiro de 2021, o objetivo desta Política é definir os princípios, diretrizes e procedimentos que visem assegurar a segurança, confidencialidade, a integridade e a disponibilidade dos dados dos sistemas corporativos e contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, em atendimento à legislação vigente, buscando informar os usuários da empresa (funcionários, contratados, terceirizados, parceiros e outros usuários autorizados) de seus requisitos obrigatórios para proteger os ativos de tecnologia e de informação da empresa. A política de segurança cibernética descreve os ativos de tecnologia e informações que devemos proteger e identifica muitas das ameaças a esses ativos.

A política de segurança cibernética também descreve as responsabilidades e os privilégios do usuário. O que é considerado uso aceitável? Quais são as regras relativas ao acesso à Internet? A política responde à essas perguntas, descreve as limitações do usuário e informa aos usuários que haverá penalidades por violação da política. Este documento também contém procedimentos para responder à incidentes que ameaçam a segurança dos sistemas de computadores e da rede da empresa. Complementar à Política de Segurança Cibernética há a Política de terceirização de serviços que contempla a contratação de serviços de processamento e armazenamento de dados de computação em nuvem.

Esta política deverá ter publicidade na Intranet da Instituição, disponibilizada aos colaboradores, assim como suas diretrizes aos fornecedores e terceirizados que possam ser afetados pelos serviços aqui mencionados.

7. QUE PROTEGEMOS:

É obrigação de todos os usuários dos sistemas da empresa proteger os ativos de tecnologia e de informação da empresa. Esta informação deve ser protegida contra acesso não autorizado, roubo e destruição. Os ativos de tecnologia e de informação da empresa são compostos pelos seguintes componentes:

· Hardware de computador, CPU, disco, e-mail, web, servidores de aplicativos, sistemas de computador, software aplicativo, software de sistema etc.

· Software do sistema, incluindo: sistemas operacionais, sistemas de gerenciamento de banco de dados e software de backup e restauração, protocolos de comunicação, sistemas legados e assim por diante.

· Software de aplicação: usado pelos vários departamentos da empresa. Isso inclui aplicativos e software personalizados e pacotes comerciais de software prontos para uso.

· Hardware e software da Rede de Comunicações, incluído: roteadores, tabelas de roteamento, hubs, modems, multiplexadores, switches, firewalls, linhas privadas e software e ferramentas de gerenciamento de rede associados.

7.1. Classificação da Informação

As informações do usuário encontradas nos arquivos e bancos de dados do sistema do computador devem ser classificadas como confidenciais ou não confidenciais. A empresa deve classificar as informações controladas por eles. O CIO deve revisar e aprovar a classificação das informações e determinar o nível de segurança apropriado para melhor protegê-las. Além disso, o CIO deve classificar as informações controladas por unidades não administradas pelo CIO.

7.2. Classificação dos Sistemas de Informação

Nível de Segurança	Descrição	Exemplo
VERMELHO	Este sistema contém informações confidenciais que não podem ser reveladas a pessoas externas à empresa. Mesmo dentro da empresa, o acesso à essas informações são fornecido na base de "necessidade de saber". O sistema fornece serviços essenciais para a missão, vitais para à operação dos negócios. A falha deste sistema pode ter consequências potencialmente fatais e / ou um impacto financeiro adverso nos negócios da empresa.	Servidor contendo dados confidenciais e outras informações do departamento em bancos de dados. Roteadores e firewalls de rede contendo tabelas de roteamento confidenciais e informações de segurança.
VERDE	Este sistema não contém informações confidenciais nem executa serviços críticos, mas fornece a	PCs do departamento de usuários usados para acessar o servidor e o(s) aplicativo(s). Estações de trabalho de

	capacidade de acessar sistemas VERMELHO através da rede.	gerenciamento usadas por sistemas e administradores de rede.
BRANCO	Este sistema não é acessível externamente. Está em um segmento de LAN isolado, incapaz de acessar sistemas VERMELHO ou VERDE. Não contém informações confidenciais nem executa serviços críticos.	Um sistema de teste usado por projetistas de sistemas e programadores para desenvolver novos sistemas de computador.
PRETO	Este sistema é acessível externamente. Ele é isolado dos sistemas RED ou GREEN por um firewall. Enquanto realiza serviços importantes, não contém informações confidenciais.	Um servidor da Web público com informações não confidenciais.

7.3. Local Area Network (LAN) Classificações

Uma LAN será classificada pelos sistemas diretamente conectados a ela. Por exemplo, se uma LAN contiver apenas um sistema VERMELHO e todos os usuários da rede estiverem sujeitos às mesmas restrições que os usuários do sistema VERMELHO systems. Uma LAN assumirá a Classificação de Segurança dos sistemas de nível mais alto anexados a ela.

8. DEFINIÇÕES:

Externamente acessível ao público. O sistema pode ser acessado via Internet por pessoas de fora da empresa, sem um ID ou senha de *logon*. O sistema pode ser acessado via conexão dial-up sem fornecer um ID de *logon* ou senha. É possível "pingar" o sistema pela Internet. O sistema pode ou não estar por trás de um firewall. Um servidor da Web público é um exemplo desse tipo de sistema.

Não público, acessível externamente. Os usuários do sistema devem ter um ID de *logon* e senha válidos. O sistema deve ter pelo menos um nível de proteção de firewall entre sua rede e à Internet. O sistema pode ser acessado pela Internet ou pela Intranet privada. Um servidor FTP privado usado para trocar arquivos com parceiros de negócios é um exemplo desse tipo de sistema.

Apenas acessível internamente. Os usuários do sistema devem ter um ID de logon e senha válidos. O sistema deve ter pelo menos dois níveis de proteção de firewall entre sua rede e à Internet. O sistema não é visível para os usuários da Internet. Pode ter um endereço de Internet privado (não traduzido) e não responde à um "ping" da Internet. Um servidor Web de intranet privado é um exemplo desse tipo de sistema.

Chief Information Officer. O Diretor do Departamento de Tecnologia da Informação (TI) atuará como Chief Information Officer (CIO).

Administrador de Segurança. Um funcionário de TI deve ser designado como Administrador de Segurança da Empresa.

9. AMEAÇAS À SEGURANÇA:

9.1. Funcionários

Uma das maiores ameaças de segurança são os funcionários. Eles podem causar danos aos seus sistemas, seja por incompetência ou de propósito. Faz-se necessário definir camadas de segurança para compensar isso também. Para atenuar a situação de ameaça, pode-se tomar as seguintes medidas:

· Somente dê direitos apropriados aos sistemas. Limitar o acesso apenas ao horário comercial.

· Não compartilhe contas para acessar sistemas. Nunca compartilhe suas informações de login com colegas de trabalho.

· Quando os funcionários são separados ou disciplinados, você remove ou limita o acesso aos sistemas.

· Avançado – Mantenha logs detalhados do Sistema em todas as atividades do computador.

· Proteja os ativos de computador com segurança física, de modo que somente funcionários com necessidades apropriadas possam acessar.

9.2. Hackers Amadores e Vândalos

Essas pessoas são o tipo mais comum de invasores na Internet. A probabilidade de ataque é extremamente alta e é provável que haja muitos ataques. Estes são geralmente crimes de oportunidade. Esses hackers amadores estão fazendo a varredura da Internet e procurando por falhas de segurança bem conhecidas que não foram conectadas. Servidores da Web e correio eletrônico são seus alvos favoritos. Uma vez que eles encontrem uma fraqueza, eles à explorarão para plantar vírus, cavalos de Tróia ou usar os recursos do seu sistema para suas intenções maliciosas. Se eles não encontrarem uma fraqueza óbvia, provavelmente passarão para um alvo mais fácil.

9.3. Hackers Criminosos e Sabotadores

A probabilidade desse tipo de ataque é baixa, mas não é totalmente improvável, dada a quantidade de informações confidenciais contidas nos bancos de dados. A habilidade desses invasores é de médio a alto, já que eles provavelmente serão

treinados no uso das mais recentes ferramentas de hackers. Os ataques são bem planejados e se baseiam em quaisquer pontos fracos descobertos que permitam a entrada na rede.

10. RESPONSABILIDADE DO USUÁRIO:

Esta seção estabelece a política de uso dos sistemas de computadores, redes e recursos de informações do escritório. Refere-se a todos os funcionários e contratados que usam os sistemas de computadores, redes e recursos de informações como parceiros de negócios e indivíduos que recebem acesso à rede para fins comerciais da empresa.

10.1. Uso Aceitável

As contas de usuário nos sistemas de computadores da empresa devem ser usadas apenas para os negócios da empresa e não devem ser usadas para atividades pessoais. O uso não autorizado do sistema pode estar violando a lei, constitui roubo e pode ser punido por lei. Portanto, o uso não autorizado do sistema de computação e das instalações da empresa pode constituir motivo para processo civil ou criminal.

Os usuários são pessoalmente responsáveis por proteger todas as informações confidenciais usadas e/ou armazenadas em suas contas. Isso inclui seus *ID's* de *logon* e senhas. Além disso, eles estão proibidos de fazer cópias não autorizadas de tais informações confidenciais e/ou distribuí-las a pessoas não autorizadas fora da empresa.

Os usuários não devem se envolver de propósito com à intenção de: assediar outros usuários; degradar o desempenho do sistema; desviar recursos do sistema para seu próprio uso; ou obter acesso a sistemas da empresa para os quais não possuem autorização.

Os usuários não devem se envolver de propósito com à intenção de: assediar outros usuários; degradar o desempenho do sistema; desviar recursos do sistema para seu próprio uso; ou obter acesso a sistemas da empresa para os quais não possuem autorização.

Os usuários são obrigados a relatar quaisquer deficiências na segurança do computador da empresa, qualquer incidente de uso indevido ou violação desta política ao seu supervisor imediato.

10.2. Uso da Internet

A empresa fornecerá acesso à Internet a funcionários e contratados conectados à rede interna e que tenham uma necessidade comercial para esse acesso. Funcionários e contratados devem obter permissão de seu supervisor e registrar uma solicitação com o Administrador de Segurança.

A Internet é uma ferramenta de negócios para a empresa. Ele deve ser usado para fins relacionados a negócios, como: comunicação via correio eletrônico com fornecedores e parceiros de negócios, obtenção de informações comerciais úteis e tópicos técnicos e comerciais relevantes.

O serviço de Internet não pode ser usado para transmitir, recuperar ou armazenar quaisquer comunicações de natureza discriminatória ou de assédio ou que sejam depreciativas para qualquer indivíduo ou grupo, obsceno ou pornográfico, ou de natureza difamatória ou ameaçadora por "correntes" ou qualquer outra finalidade que é ilegal ou para ganho pessoal.

10.3. Classificação do usuário

Todos os usuários devem ter conhecimento dessas políticas de segurança e devem informar violações ao Administrador de Segurança. Além disso, todos os usuários devem estar em conformidade com a Política de uso aceitável definida neste documento. A empresa estabeleceu os seguintes grupos de usuários e definiu os privilégios e responsabilidades de acesso:

Categoria do usuário	Privilégios e Responsabilidades
Usuários do Departamento (Funcionários)	Acesso à aplicativos e bancos de dados, conforme necessário para a função de trabalho (VERMELHO E /ou VERDE apurado).
Administradores de Sistema	Acesso a sistemas de computadores, roteadores, hubs e outras tecnologias de infraestrutura necessárias para o trabalho. Acesso a informações confidenciais apenas com base em "necessidade de saber".
Administrador de Segurança	Maior nível de segurança. Acesso permitido a todos os sistemas de computadores, bancos de dados, firewalls e dispositivos de rede, conforme necessário para a função de trabalho.
Analistas de TI /Programador	Acesso à aplicativos e bancos de dados conforme necessário para uma função de trabalho específica. Não autorizado a acessar roteadores, firewalls ou outros dispositivos de rede.
Contratados/Consultores	Acesso à aplicativos e bancos de dados, conforme necessário para funções de trabalho específicas. Acesso a roteadores e firewall somente se necessário para a função job. Conhecimento de políticas

	de segurança. O acesso à informações e sistemas da empresa deve ser aprovado por escrito pelo diretor / CEO da empresa.
Outras agências e parceiros de negócios	Acesso à aplicativos e bancos de dados, conforme necessário para funções de trabalho específicas. Acesso a roteadores e firewall somente se necessário para a função job. Conhecimento de políticas de segurança. O acesso à informações e sistemas da empresa deve ser aprovado por escrito pelo diretor / CEO da empresa.
Público Geral	O acesso é limitado à aplicativos executados em servidores da Web públicos. O público em geral não terá permissão para acessar informações confidenciais.

10.4. Monitoramento do Uso de Sistemas de Computação

A empresa tem o direito e a capacidade de monitorar informações eletrônicas criadas e/ou comunicadas por pessoas que usam sistemas e redes de computadores da empresa, incluindo mensagens de e-mail e uso da Internet. Não é política ou intenção da empresa monitorar continuamente todo o uso do computador por funcionários ou outros usuários dos sistemas de computadores e da rede da empresa. No entanto, os usuários dos sistemas devem estar cientes de que a empresa pode monitorar o uso, incluindo, mas não limitado a padrões de uso da Internet (por exemplo, acesso ao site, duração on-line, horário de acesso) e arquivos eletrônicos dos funcionários e mensagens na medida necessária para assegurar que à Internet e outras comunicações eletrônicas estejam sendo usadas em conformidade com a lei e com a política da empresa.

11. CONTROLE DE ACESSO:

Um componente fundamental da nossa política de segurança cibernética é o controle do acesso aos recursos de informações críticas que exigem proteção contra divulgação ou modificação não autorizada. O significado fundamental do controle de acesso é que as permissões são atribuídas a indivíduos ou sistemas que estão autorizados a acessar recursos específicos. Controles de acesso existem em várias camadas do sistema, incluindo a rede. O controle de acesso é implementado pelo ID de *logon* e pela senha. No nível do aplicativo e do banco de dados, outros métodos de controle de acesso podem ser implementados para restringir ainda mais o acesso. O aplicativo e os sistemas de banco de dados podem limitar o número de aplicativos e bancos de dados disponíveis para os usuários com base em seus requisitos de trabalho.

11.1. Sistemas de usuários e Acesso à Rede – Identificação Normal do Usuário

Todos os usuários deverão ter um ID de *logon* e senha exclusivos para acesso aos sistemas. A senha do usuário deve ser mantida em sigilo e NÃO DEVE ser compartilhada com o pessoal de gerenciamento e supervisão e/ou com qualquer outro funcionário. Todos os usuários devem cumprir as seguintes regras referentes à criação e manutenção de senhas:

· A senha não deve ser encontrada em nenhum dicionário em inglês ou no estrangeiro. Ou seja, não use nenhum nome, substantivo, verbo, advérbio ou adjetivo comum. Estes podem ser facilmente quebrados usando “ferramentas de hackers” padrão.

· As senhas não devem ser postadas em terminais de computador ou perto dele ou de outra forma estar prontamente acessíveis na área do terminal.

· A senha deve ser alterada a cada (45 dias).

· As contas de usuários serão congeladas após (60 dias) tentativas de login sem sucesso.

· IDs e senhas de *logon* serão suspensos após (60 dias) de uso.

Os usuários não têm permissão para acessar arquivos de senha em nenhum componente da infraestrutura de rede. Os arquivos de senhas nos servidores serão monitorados para acesso por usuários não autorizados. Copiar, ler, excluir ou modificar um arquivo de senha em qualquer sistema de computador é proibido.

Os usuários não poderão fazer *logon* como administrador do sistema. Os usuários que precisam desse nível de acesso aos sistemas de produção devem solicitar uma conta de acesso especial, conforme descrito em outras partes deste documento.

Os IDs e senhas de *logon* dos funcionários serão desativados assim que possível, se o funcionário for demitido, demitido, suspenso, demitido ou deixar o emprego do escritório da empresa.

Os supervisores/gerentes devem entrar em contato direto e imediato com o gerente de TI da empresa para relatar a mudança no status do funcionário que exija o cancelamento ou a modificação dos privilégios de acesso de *logon* do funcionário.

Os funcionários que esquecerem sua senha devem ligar para o departamento de TI para obter uma nova senha atribuída a sua conta. O funcionário deve identificar-se pela matrícula para o departamento de TI.

Os funcionários serão responsáveis por todas as transações que ocorrem durante as sessões de *logon* iniciadas pelo uso da senha e do ID do funcionário. Os funcionários não devem fazer *logon* em um computador e permitir que outro indivíduo use o computador ou compartilhe o acesso aos sistemas do computador.

11.2. Acesso do Administrador do Sistema

Administradores de sistema, administradores de rede e administradores de segurança terão acesso (tipo de acesso) a sistemas host, roteadores, hubs e firewalls, conforme necessário para cumprir as obrigações de seu trabalho.

Todas as senhas do administrador do sistema serão EXCLUÍDAS imediatamente depois que qualquer funcionário que tenha acesso a essas senhas for demitido, ou de outra forma, deixar o emprego da empresa.

Apenas o administrador de sistemas e o CIO estão autorizados a entrar na sala de servidores, a não ser em caso excepcional, seja pelo não comparecimento do administrador de sistemas e do CIO na instituição, poderá ser feito por outro profissional da área de TI lotado na Coordenadoria de Informática. Nos casos de manutenção de equipamentos dentro da sala de servidores, profissionais externos poderão acessar, desde que acompanhados por pessoal autorizado.

11.3. Acesso Especial

Contas de acesso especiais são fornecidas a indivíduos que exigem privilégios temporários de administrador do sistema para executar seu trabalho. Essas contas são monitoradas pela empresa e exigem a permissão do gerente de TI da empresa do usuário. O monitoramento das contas especiais de acesso é feito inserindo os usuários em uma área específica e periodicamente gerando relatórios para o gerenciamento. Os relatórios mostrarão quem tem atualmente uma conta de acesso especial, por que motivo e quando expirará. As contas especiais expiram em (X # de) dias e não serão automaticamente renovadas sem permissão por escrito.

11.4. Conectando-se a redes de terceiros

Essa política é estabelecida para garantir um método seguro de conectividade fornecido entre a empresa e todas as empresas de terceiros e outras entidades necessárias para trocar informações eletronicamente com a empresa.

“Terceiros” refere-se a fornecedores, consultores e parceiros de negócios que fazem negócios com a empresa e outros parceiros que precisam trocar informações com a empresa. Conexões de rede de terceiros devem ser usadas somente pelos funcionários de terceiros, apenas para fins comerciais da empresa. A empresa terceirizada garantirá que somente usuários autorizados terão permissão para acessar informações na rede da empresa. O terceiro não permitirá que o tráfego da Internet ou outro tráfego de rede privada flua para a rede. Uma conexão de rede de terceiros é definida como uma das seguintes opções de conectividade:

· Uma conexão de rede terminará em um (a ser especificado) e o terceiro estará sujeito às regras padrão de autenticação da empresa.

Esta política se aplica a todas as solicitações de conexão de terceiros e a quaisquer conexões de terceiros existentes. Nos casos em que as conexões de rede de terceiros existentes não atenderem aos requisitos descritos neste documento, elas serão reprojetadas conforme necessário.

Todas as solicitações de conexões de terceiros devem ser feitas enviando uma solicitação por escrito e sendo aprovadas pela empresa.

11.5. Conectando Dispositivos à Rede

Somente dispositivos autorizados podem estar conectados à (s) rede (s) da empresa. Dispositivos autorizados incluem PCs e estações de trabalho de propriedade da empresa que cumprem as diretrizes de configuração da empresa. Outros dispositivos autorizados incluem dispositivos de infraestrutura de rede usados para gerenciamento e monitoramento de rede.

Os usuários não devem se conectar à rede: computadores que não sejam da empresa e que não sejam autorizados, de propriedade e / ou controlados pela empresa. Os usuários são especificamente proibidos de especificar à rede da empresa.

OBSERVAÇÃO: os usuários não estão autorizados a conectar qualquer dispositivo que altere as características de topologia da rede ou de dispositivos de armazenamento não autorizados, por exemplo, pen drives e CDs graváveis.

11.6. Acesso Remoto

Somente pessoas autorizadas podem acessar remotamente a rede da empresa. O acesso remoto é fornecido aos funcionários, contratados e parceiros de negócios da empresa que têm uma necessidade comercial legítima de trocar informações, copiar arquivos ou programas ou acessar aplicativos de computador. A conexão autorizada pode ser um PC remoto para a rede ou uma rede remota para a conexão de rede da empresa. O único método aceitável de se conectar remotamente à rede interna é usar um ID seguro.

11.7. Acesso Remoto Não Autorizado

A ligação de (por exemplo, hubs) a um PC ou estação de trabalho de um usuário que esteja conectado à LAN da empresa não é permitida sem a permissão por escrito da empresa. Além disso, os usuários não podem instalar software pessoal projetado para fornecer controle remoto do PC ou da estação de trabalho. Esse tipo de acesso remoto ignora os métodos altamente seguros autorizados de acesso remoto e representa uma ameaça à segurança de toda a rede.

12. DETALHAMENTO:

12.1. Considerações iniciais

A diretoria responsável por esta política é a Diretoria Administrativa e Financeira (DIRAF). A gerência responsável pela manutenção dessa política é a Gerência de Tecnologia da Informação (GETEC), que avaliará casos omissos, e pautará para apreciação da DIRAF, se entender necessário.

12.2. Incidentes Relevantes

São considerados incidentes relevantes, aqueles que afetam o core business do GoiásFomento, ou seja, que impactam nas atividades de entrega, ou interrompem os serviços de maneira sistêmica.

Ocorrendo um incidente relevante, deverá ser realizado o registro, análise das causas e dos impactos, bem como dos controles existentes, mantendo esses registros disponíveis pelo prazo de 05 (cinco) anos.

Devem ter o mesmo tratamento incidentes relevantes ocorridos em empresas prestadoras de serviço.

12.2.1. Registro de Demandas

Quaisquer demandas à GETEC (incidentes ou não) devem ser encaminhadas através de um chamado para que a GETEC verifique, e proceda com o atendimento, o que pode envolver empresas prestadoras de serviço, ou a orientação necessária.

Todos os chamados deverão ser abertos através de ferramenta definida pela GETEC, que fará o gerenciamento das demandas recebidas.

12.3. Classificação

A descrição e classificação detalhada dos Serviços relevantes prestados por terceiros é também parte integrante do Plano de Continuidade de Negócios:

Serviço	Empresa	Estratégia Alternativa	Tolerância à Interrupção
Links de acesso para comunicação com a Internet	G8 (Superi)	A alternativa implantada visa atender processos críticos que podem gerar multas ou penalidades e dependem do recurso, a instituição dispõe de 3 modens 4G habilitados para atender em regime de contingência.	Até 8h
Solução $Finance (Serviços de desenvolvimento e manutenção de sistemas)	Sinqia	Como a empresa atua fora da GoiásFomento, pode ocorrer algum problema na comunicação entre as empresas, impedindo o recebimento ou entrega de demandas. Nesse caso, a contingência seria permitir a alteração da data da entrega, ou mesmo receber os técnicos no GoiásFomento, para conclusão da atividade.	Até 8h
Serviços de locação de impressoras e scanners		As impressões podem ser direcionadas para outros dispositivos.	Até 8h

13. PENALIDADE POR VIOLAÇÃO DE SEGURANÇA:

A empresa leva a questão da segurança a sério. As pessoas que usam os recursos de tecnologia e informação da empresa devem estar cientes de que podem ser disciplinadas se violarem essa política. **Em caso de violação desta política, um funcionário da empresa pode estar sujeito a medidas disciplinares.** A disciplina específica imposta será determinada caso a caso, levando em consideração a natureza e a gravidade da violação da Política de Segurança Cibernética, violações anteriores da política cometida pelas leis individuais, estaduais e federais e todas as outras leis relevantes em formação. A disciplina que pode ser tomada contra um funcionário deve ser administrada de acordo com as regras ou políticas apropriadas e com o Manual de Normas da empresa.

Em um caso em que o acusado não é um funcionário da empresa, o assunto deve ser submetido ao CIO. O CIO pode encaminhar as informações para que o RH a fim de efetuar a aplicação da lei e/ou para representação de acusações criminais contra o(s) alegado(s) infrator (es).

14. PROCEDIMENTOS DE MANUSEIO DE INCIDENTES DE SEGURANÇA:

14.1. Esta seção fornece algumas diretrizes e procedimentos de políticas para lidar com incidentes de segurança. O termo “incidente de segurança” é definido como qualquer evento irregular ou adverso que ameace a segurança, integridade ou disponibilidade dos recursos de informação em qualquer parte da rede da empresa. Alguns exemplos de incidentes de segurança são:

· Acesso ilegal de um sistema de computador da empresa. Por exemplo, um hacker faz *logon* em um servidor de produção e copia o arquivo de senha.

· Danos ao sistema de computador ou rede da empresa causados por acesso ilegal. Liberar um vírus ou *worm* seria um exemplo.

· Ataque de negação de serviço contra um servidor da web da empresa. Por exemplo, um hacker inicia uma enxurrada de pacotes contra um servidor da Web projetado para causar falhas no sistema.

· Uso malicioso de recursos do sistema para iniciar um ataque contra outro computador fora da rede da empresa. Por exemplo, o administrador do sistema percebe uma conexão com uma rede desconhecida e um processo estranho acumulando muito tempo do servidor.

Os funcionários, que acreditam que seus sistemas de terminal ou computador tenham sido submetidos à um incidente de segurança, ou que tenham sido acessados ou usados de maneira inadequada, devem comunicar a situação imediatamente ao (seu representante). O funcionário não deve desligar o computador ou excluir arquivos suspeitos. Deixar o

computador na condição em que estava quando o incidente de segurança foi descoberto ajudará a identificar à origem do problema e a determinar as etapas que devem ser tomadas para solucionar o problema.

Os critérios relacionados à contratação de serviços de processamento e armazenamento de dados de computação em nuvem constam da política de terceirização de serviços.

14.2. Serviços e incidentes passíveis de interrupção

Abaixo são listados alguns serviços passíveis de interrupção em complemento aos descritos no Plano de Continuidade de Negócios.

Serviço	Incidente	Comunicação	Possíveis causas	Ação	Prazo para início do Atendimento	Estratégia de Continuidade	Plano de Recuperação
Dados contidos nos Sistemas de Banco de dados no Data Center	Há uma interrupção do serviço de hospedagem do Banco de Dados no Data Center na SEDI (Secretaria de Estado de Desenvolvimento e Inovação).	A GETEC informará os usuários da interrupção dos serviços através da ferramenta Teams. A GETEC comunicará a Gerência de Riscos Corporativos do incidente e suas implicações.	1 – Manutenção nos servidores do DataCenter 2 – Regulamentação do serviço.	O Analista da GETEC deverá avaliar junto ao contato na SEDI qual o período previsto dessa interrupção e escolher a estratégia de continuidade.	Imediato	-Até 4 horas de interrupção: Aguardar o retorno do serviço; -Até 8 horas de interrupção: Avaliar restaurar o último backup válido em servidor interno enquanto aguarda o retorno do serviço; -Acima de 8 horas de interrupção: Restaurar último backup válido em servidor interno e disponibilizar para os usuários.	Deverá ser avaliado a depender do incidente.
Dados e Informações de usuários colaboradores e/ou de clientes da Instituição	Vazamento de Dados protegidos por lei, a exemplo da LGPD e da Lei do sigilo bancário.	Quando identificado o incidente deverá ser comunicado à GETEC.	1- O usuário encaminhou e-mail contendo relatório de operações de clientes para terceiros; 2- O usuário utilizou de ferramentas da empresa para efetuar consultas para fins particulares.	A GETEC colherá as evidências possíveis nos sistemas caso existam, incluindo logs de auditoria, logs de acesso e comunicará ao Comitê Setorial de Compliance e ao DPO (Data Protection Officer) que fará a avaliação e comunicação à ANPD (Autoridade Nacional de Proteção de Dados) e ao Banco Central do Brasil.	Imediato		Caberá ao Comitê Setorial de Compliance e ao DPO definir as próximas medidas a serem tomadas de acordo com a situação.
Dados e ferramentas utilizados pelo usuário para execução de suas atividades	O computador foi infectado por ameaças do tipo: Vírus, Trojan, Worms, keylogger ou outro tipo de ameaça.	O usuário deverá entrar em contato com a GETEC pelos números 3216-4978 /3216-4973 /3216-5020 ou por e-mail getec@goiasfomento.com relatando o ocorrido.	3- O computador foi infectado após clique em link suspeito 4- O computador foi infectado após uso de pen-drive infectado	O Analista da GETEC deverá iniciar o atendimento avaliando retirando o computador da rede afim de evitar que outras máquinas sejam afetadas.	30 minutos	1 - Orientar o colaborador a utilizar outra estação de trabalho pois as permissões estão vinculadas ao seu usuário de rede;	1- Efetuar o backup seguro dos dados e formatar o computador.

			5- O computador foi infectado após download e execução de arquivo infectado.				
Dados contidos nos Sistemas de Banco de dados.	O acesso aos dados dos sistemas não é permitido devido a uma falha de hardware ou de software.	O usuário deverá entrar em contato com a GETEC pelos números 3216-4978 /3216-4973 /3216-5020 ou por e-mail getec@goiasfomento.com relatando o ocorrido.	1- O computador do usuário está com falha na conexão de rede; 2- O usuário não recorda sua senha; 3- O usuário não tem permissão para acessar aquele recurso; 4- Há uma falha na conexão de rede do servidor no qual está o Banco de Dados; 5- Há uma falha na conexão de rede do servidor na qual está instalada a aplicação.	O Analista da GETEC deverá iniciar o atendimento avaliando se a indisponibilidade é local (no computador do usuário) ou geral (nos demais computadores da instituição).	30 minutos	1 - Orientar o colaborador a utilizar outra estação de trabalho pois as permissões estão vinculadas ao seu usuário de rede; 2 – Confirmar a identidade do colaborador, gerar uma nova senha temporária e solicitar que seja alterada; 3- Validar com o Gerente da área se o colaborador deve ter acesso aos dados, em caso afirmativo conceder as permissões. 4/5 – Comunicar ao demais usuários através da ferramenta Teams da indisponibilidade do serviço;	1- Caso seja uma falha de hardware no computador efetuar a substituição. Sendo falha no ponto de rede, comunicar a GEPAT (responsável pela gestão do contrato de manutenção na rede física). 4/5 – Abrir chamado junto ao fornecedor do serviço. Acompanhar o chamado de acordo com o SLA.
Link de Internet	Não há serviço de internet disponível, ou o carregamento de sites, download arquivos está muito lento, impactando as operações dos usuários.	O usuário deverá entrar em contato com a GETEC pelos números 3216-4978 /3216-4973 /3216-5020 ou por e-mail getec@goiasfomento.com relatando o ocorrido.	1 - O computador do usuário está com falha na conexão de rede; 2 – Há uma falha na conexão (link de internet) da Instituição; 3 – O site que o usuário está tentando acessar está indisponível.	O Analista da GETEC deverá iniciar o atendimento avaliando se a indisponibilidade é no site utilizado (o teste pode ser realizado com uma conexão 4g) , ou local (no computador do usuário) ou geral (nos demais computadores da instituição).	15 minutos	1 - Orientar o colaborador a utilizar outra estação de trabalho pois as permissões estão vinculadas ao seu usuário de rede; 2 – Comunicar aos gerentes de áreas por telefone, da indisponibilidade do serviço; 3 – Comunicar ao usuário da indisponibilidade do site.	1-Caso seja uma falha de hardware no computador efetuar a substituição. Sendo falha no ponto de rede, comunicar a GEPAT (responsável pela gestão do contrato de manutenção na rede física). 2 – Abrir chamado junto ao fornecedor do serviço. Acompanhar o chamado de acordo com o SLA.

14.3. Procedimentos de Comunicação

Os incidentes considerados relevantes serão comunicados pela Gerência de Tecnologia através de processo criado no Sistema Eletrônico de Informações (sei.go.gov.br) ao Comitê Setorial de Compliance e ao DPO (Data Protection Officer). Estes farão a avaliação e comunicação ao Banco Central do Brasil em até 30 após a identificação do incidente.

Em caso de incidente relevante envolvendo vazamento de dados o Comitê Setorial de Compliance e o DPO (Data Protection Officer) deverão fazer comunicação também à ANPD (Autoridade Nacional de Proteção de Dados).

A comunicação deverá conter no mínimo os seguintes dados:

· A descrição da natureza dos dados pessoais afetados;

· As informações sobre os titulares envolvidos;

· A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

· Os riscos relacionados ao incidente;

· Os motivos da demora, no caso de a comunicação não ter sido imediata; e

· As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Havendo necessidade, as informações sobre incidentes relevantes poderão ser compartilhadas com outras instituições financeiras, ou demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Goiânia (GO), 14 de junho de 2023.

Documento assinado eletronicamente por **EURIPEDES JOSE DO CARMO**, **Presidente**, em 04/08/2023, às 15:05, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

Documento assinado eletronicamente por **LEANDRA ADRIANO DE ASSIS**, **Diretor (a)**, em 04/08/2023, às 16:20, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

Documento assinado eletronicamente por **LUCAS FERNANDES DE ANDRADE**, **Diretor**, em 07/08/2023, às 12:08, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **49532668** e o código CRC **888B21DF**.