POLÍTICA DE CONTINUIDADE DE NEGÓCIOS (PCN)

Glossário

AIN - Análise de Impacto para o Negócio

CCN - Comitê de Continuidade de Negócios

OMC - Objetivo Mínimo de Continuidade

PCN - Plano de Continuidade de Negócios

PRI - Plano de Resposta a Incidentes

PSI - Política de Segurança da Informação

TRI - Time de Resposta a Incidentes

1. Objetivo

a. Seguindo as disposições da PSI estabelecem-se aqui as regras e procedimentos relacionados à atividade de Continuidade de Negócios no ambiente da VIACERTA.

b. As diretrizes gerais sobre o PCN estão presentes no capítulo 11 da PSI da VIACERTA, que deve ser considerada como complementar a esta PCN.

2. Da sua Aplicação

a. A aprovação desta Política é realizada nos âmbitos da Instituição pelos respectivos órgãos de administração (Conselho de Administração e/ou Diretoria).

    i. O Gestor de Segurança da Informação é o responsável geral pela execução, revisão e testes do presente plano.

b. Com base no Inventário de Ativos mantidos na instituição, assim determinado pela PSI, é realizada a AIN dos processos de negócio cujo escopo está abrangido por esta PCN.

c. A AIN leva em consideração quais os ativos de suporte e infraestrutura que mantém cada um dos processos de negócio avaliados. Também são determinados os tempos de indisponibilidade aceitáveis para cada processo e os recursos necessários para a ativação desta PCN.

i. Levando em conta os índices de disponibilidade apontados para cada um dos serviços, foram estipulados tempos máximos de normalização do funcionamento, sempre levando-se em conta o índice mais alto em cada um dos cenários previstos.

ii. Neste sentido, optou-se por adotar o tempo de indisponibilidade por base mensal, tempo este que será o máximo objetivado, no mês em questão, para o reinício dos serviços.

iii. Os procedimentos adotados nesta PCN visam atender ao OMC, ou seja, o mínimo de serviços que deve estar operacional para a prestação dos serviços.

d. A partir dos resultados da análise de riscos e/ou por determinação do Conselho de Administração e na sua ausência pela Diretoria, cada área identifica processos ou atividades críticas para os quais são definidas estratégias e construídos planos de continuidade de negócios, considerando:

i. Ameaças e vulnerabilidades das situações analisadas;

ii. probabilidades e impactos que envolvam a indisponibilidade dos processos de negócio analisados, bem como a avaliação dos riscos;

iii. estratégias de continuidade e custos de implementação;

iv. consequências de não se implementar mecanismos de contingência (perdas potenciais);

v. os recursos essenciais relacionados a pessoas, instalações, tecnologias, informações, suprimentos e partes interessadas (stakeholders) e serviços relevantes prestados por terceiros;

vi. Para os recursos essenciais, são formalmente estabelecidos os planos com procedimentos alternativos para recuperação das atividades exigidas, no tempo desejado, observada a relação custo e/ou benefício e o impacto potencial.

e. Esta PCN é aplicável aos negócios considerados críticos pelos órgãos de administração das entidades da VIACERTA, em função de potenciais impactos negativos, financeiros, patrimoniais, legais, regulatórios e de imagem.

f. Conforme o item anterior, como escopo desta PCN, os seguintes processos de negócio são por ela cobertos:

i. Processo Comercial; Processo de Cobrança; Processo de Repasses; Processo Administrativo Financeiro; Processo de Análise

de Crédito; Processamento de Dados; Processo de Recursos Humanos; Processo Cobrança Assessorias; Processo Call Center; Processo Departamento Pessoal.

ii. Adicionalmente, também é levado em consideração neste escopo o funcionamento da operação da instituição em sua sede principal em caso de sua indisponibilidade (Perda da Sede Principal da Instituição).

g. Os procedimentos de continuidade de negócios, que estão apresentados nesta política, são objetivos, concisos, prevendo o processo em que cada plano deve ser utilizado, os responsáveis pelos procedimentos de recuperação e os procedimentos que serão executados para a contingência ou a recuperação dos recursos que sofreram interrupção.

h. A presente política deverá ser impressa e entregue aos responsáveis pela sua implementação para ser utilizada no caso de perda do acesso digital à mesma, além de sua disponibilização em ambiente de nuvem seguro e acessível via VPN por todos os envolvidos.

3. Da Gestão de Continuidade

a. A presente política leva em consideração o cenário de negócios no qual a VIACERTA está inserida e as disposições legais aplicáveis (como a Resolução n. 4.658/2018 do BACEN e a Lei Geral de Proteção de Dados Pessoais - Lei 13.709/2018).

b. Os requisitos para modelagem da PCN são estabelecidos por meio da atividade de análise de risco, atividade esta promovida de maneira contínua na instituição pela equipe de Segurança da Informação. Na ocorrência de incidentes relevantes, alterações no cenário, reconhecimento de novas vulnerabilidades ou modalidades de ataques, a análise de risco é atualizada refletindo, assim, os procedimentos necessários de controle.

c. Com base no processo de gestão e avaliação de riscos (conforme a PSI), quando da identificação de novas atividades ou implementação de novos ativos que estejam relacionados ao escopo desta PCN, ela deverá ser atualizada para fazer constar as atividades que cubram as modificações implementadas no ambiente.

d. O processo de análise de risco com o foco em continuidade levará em consideração os seguintes requisitos:

i. A identificação dos riscos que afetem processos de negócio a serem cobertos pela PCN;

ii. A identificação da probabilidade de ocorrência do referido risco e o impacto para a instituição, conforme a AIN.

iii. A identificação dos tempos objetivados de recuperação.

e. A definição dos tempos de indisponibilidade aceitáveis para cada um dos processos de negócio foram assim definidos por meio da AIN realizada pela instituição. Tais tempos guiam as atividades de continuidade.

f. A gestão da continuidade de negócios é objeto de acompanhamento sistemático por parte dos órgãos de administração da instituição.

4. Descrição Geral dos Meios de Contingência

a. A VIACERTA utiliza a nuvem da Azure, com infraestrutura alternativa de contingência em localização distinta da principal, assim criada e mantida com base na análise de risco realizada. Nesse sentido, o ambiente de nuvem está preparado e configurado com mecanismos de contingência, continuidade e *disaster recovery* com base neste PCN e também no Plano de Recuperação de Desastre de Data Center.

b. Existem dois links de acesso à Internet na sede da instituição fornecidos por duas empresas com infraestruturas independentes, atualmente sendo Oi e Sygo.

c. Em face dos efeitos da pandemia de Covid-19, a VIACERTA pôde testar com sucesso os meios e medidas para que os funcionários pudessem desempenhar suas atividades de suas residências. Todos os setores tiveram funcionários trabalhando em *home office* durante a pandemia, inclusive o atendimento ao cliente. Neste sentido, a instituição está devidamente preparada para a realização de atividades de maneira emergencial por este meio, em caso de indisponibilidade de sua sede central.

d. A Política de Backup da instituição, sumariamente, está assim organizada:

i. Data Center Santo Cristo:

1. Para os backups de Infraestrutura do FileServer, é utilizado o agente de ArcServe para gerar os pontos de recuperação.

2. No caso das VMs, os agentes estão instalados nos Hypervisors, permitindo a replicação total da VM para o servidor de backup.

ii. Teste de Restore

1. Fileserver: Toda semana é testado o restore de algum arquivo para validar o funcionamento do sistema.

2. Máquinas Virtuais: A cada 3 meses é efetuada restauração de uma VM completa sem rede, e são validados os arquivos e sistemas de maneira isolada.

iii. Azure:

1. Para VMs com Sistema Operacional Windows, o backup ocorre de maneira nativa e automática, sem utilização de agentes ou software adicional.

2. No caso de VMs com Sistema Operacional Linux, é instalado o agente disponibilizado pela Microsoft para o correto funcionamento do processo de backup.

iv. Teste de Restore:

1. Máquinas Virtuais: A cada 3 meses é efetuado o restore de uma VM completa com *Network Security Group* (NSG) restrito, e são validados os arquivos e sistemas de maneira isolada.

v. Bancos de Dados: Todo dia é efetuado um restore do Banco de Dados de produção para o ambiente de testes, consideramos este restore um teste integral do backup.

e. As medidas de contingência e continuidade aqui planejadas, em face da utilização de recursos de nuvem, podem ser ativadas à distância, quando necessário. Para isso, há estrutura específica de VPNs para os acessos aos recursos necessários e os funcionários responsáveis sempre portam notebooks da instituição. Além do mais, a VIACERTA possui uma sede alternativa para situações de comprometimento de sua sede principal, localizada a uma quadra de distância. Neste sentido, ações de continuidade que envolvem o comprometimento da sede principal podem ser facilmente tomadas na sede auxiliar da instituição.

f. Como meio de controle de incidentes e possível escalação da PCN, a VIACERTA mantém um TRI que realiza a categorização e classificação de incidentes. Além das tarefas gerais de resposta a incidentes, o referido time também pode escalar um incidente, visando a ativação do plano de

continuidade, quando as primeiras respostas demonstrarem sua necessidade.

i. Esta atividade utiliza sistemas específicos de registro de incidentes, categorização e classificação. Conforme o própria Plano de Ação e Resposta a Incidentes, os incidentes de “Nível 4 - Emergencial”, quando não resolvidos no tempo previsto, ou seja, perdido o controle sobre o seu gerenciamento, devem ser escalados para situação de crise, que levará a ativação do PCN, quando os serviços envolvidos estiverem cobertos por este plano.

5. Ativação do Plano

a. O plano será ativado nas seguintes situações:

   i. Quando, por meio de entradas realizadas no TRI, detectar-se a afetação na disponibilidade de um recurso necessário para a prestação dos serviços da instituição, conforme a projeção da complexidade e afetação de ativos que suportem os processos de negócio controlados por este plano.

      1. Em tais casos, ao se detectar uma situação que não possa ser adequadamente controlada, levando em consideração os tempos aceitáveis de indisponibilidade para cada serviço, o TRI escalará o incidente para ser tratado por meio desta política.

      2. Na situação acima, o plano somente será ativado quando as medidas de contingência forem impossíveis de serem realizadas em tempo menor do que o aceitável da indisponibilidade do processo de negócio. Neste sentido, o TRI projetará o tempo de resolução do incidente.

b. Quando os mecanismos de monitoramento dos ativos que mantém os serviços prestados pela instituição dispararem alertas que indiquem, pela sua gravidade, a impossibilidade de recuperação dos ativos nos tempos esperados para o controle de incidentes.

c. Quando o incidente, pela sua gravidade e reconhecimento de complexidade, puder ser imediatamente reconhecido como apto a ser tratado diretamente pela PCN (como, por exemplo, um incidente grave que afete a sede da VIACERTA).

d. Em todas as situações acima, a decisão sobre ativar ou não a PCN cabe ao Comitê de Continuidade de Negócios (CCN).

6. Da Revisão e Testes

a. Esta política é revisada, no mínimo, anualmente ou, ainda, por proposta da área responsável pelo gerenciamento do risco operacional da VIACERTA Financiadora ou em decorrência de fatos relevantes que demonstrem sua ineficácia.

b. Pelo menos uma vez por ano, os procedimentos previstos nesta política serão submetidos a testes documentados de sua eficácia. Neste momento, as equipes envolvidas também colocarão em prática, como exercícios, as atividades aqui previstas.

7. Considerações Finais

a. Complementam esta política e a ela se subordinam todas as normas e procedimentos operacionais que regulam a gestão da continuidade de negócios, no âmbito da VIACERTA Financiadora.

b. O PRI possui, em seu cap. 3, as diretrizes acerca da notificação e compartilhamento sobre informações relevantes, que será observado, inclusive, quando da ocorrência de incidentes que promovam a informação sobre as ativações emergenciais deste PCN.

8. Procedimentos do Plano de Continuidade

8. 1 - Ataque de Negação de Serviço Contra a Infraestrutura do Provedor

Resultado da Análise de risco		
Probabilidade: Média	**Impacto: Médio**	**Risco: Médio**

Descrição da ameaça:	Ataque de negação de serviço contra a infraestrutura do provedor de nuvem via Internet, tipicamente DDoS (Distributed Denial of Service). Não são considerados ataques à estrutura física do provedor.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Rafael Angst: Gestor de Segurança da Informação (55) 9934-9920

Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Jaime Zimmer: Analista de Infraestrutura (55) 99952-6191
Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de TI Donos dos Processos
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Recursos da nuvem que possuem IP público. “Inventário de Ativos.xlsx”
Recursos de Infraestrutura de contingência para o funcionamento do processo:	Ambiente de Disaster Recovery (Azure EUA).
Procedimentos:	Ativar o Plano de Recuperação de Desastre (DR) - “OP_0001_00 - Plano de Recuperação de Desastre de Data Center.docx” levando em consideração os seguintes procedimentos: 1. IT_0001_00 - Start de Banco de Dados no ambiente de DR.docx 2. IT_0002_00 - Garantir o processo de conectividade no ambiente de DR.docx 3. IT_0003_00 - Alterações de DNS Externo para Ambiente de DR.docx 4. IT_0004_00 - Alterações em Servidores WEB para Ambiente de DR.docx 5. IT_0005-00 _ Alterações em Servidores RDS para ambiente de DR.docx 6. IT_0006-00 _ Alterações em Servidores APP para ambiente de DR.docx 7. IT_0007-00 _ Alterações no Servidor de Arquivos para ambiente de DR.docx 8. IT_0008_00 - Start de Banco de Dados no ambiente de DR - POSTGRESQL.docx 9. IT_0010_00 - Validação de Sistemas para ambiente de DR.docx 10. IT_0011_00 - Validação de Sistemas para ambiente de DR.docx 11. IT_0012_00 - Alterações ConnectDirect.docx
Tempos objetivados de recuperação (base mensal)	Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS (PCN)

8.2 - Ataque de Negação de Serviço Contra um Ativo Específico

Resultado da Análise de risco		
Probabilidade: Alta	**Impacto: Médio**	**Risco: Alto**

Descrição da ameaça:	Ataque de negação de serviço contra servidores/serviços da VIACERTA hospedados no provedor em nuvem. São considerados ataques direcionados visando esgotar capacidade dos servidores ou ainda esgotar limites de serviços das aplicações.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Jaime Zimmer - Analista de Infraestrutura (55) 99952-619
Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Guillermo Elía - Analista de Infraestrutura (55) 99713-6568

Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Coordenador de Infraestrutura de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Ativos de Suporte e Infraestrutura. “Inventário de Ativos.xlsx”
Recursos de Infraestrutura de contingência para o funcionamento do processo:	Os servidores/serviços possuem recursos de contingência. Ambiente de Disaster Recovery (Azure EUA).
Procedimentos:	1 - Ativar servidores/serviços de contingência. 2 - “OP_0001_00 - Plano de Recuperação de Desastre de Data Center.docx” levando em consideração os seguintes procedimentos: 12. IT_0001_00 - Start de Banco de Dados no ambiente de DR.docx 13. IT_0002_00 - Garantir o processo de conectividade no ambiente de DR.docx 14. IT_0003_00 - Alterações de DNS Externo para Ambiente de DR.docx 15. IT_0004_00 - Alterações em Servidores WEB para Ambiente de DR.docx 16. IT_0005-00 _ Alterações em Servidores RDS para ambiente de DR.docx 17. IT_0006-00 _ Alterações em Servidores APP para ambiente de DR.docx 18. IT_0007-00 _ Alterações no Servidor de Arquivos para ambiente de DR.docx 19. IT_0008_00 - Start de Banco de Dados no ambiente de DR - POSTGRESQL.docx 20. IT_0010_00 - Validação de Sistemas para ambiente de DR.docx 21. IT_0011_00 - Validação de Sistemas para ambiente de DR.docx 22. IT_0012_00 - Alterações ConnectDirect.docx
Tempos objetivados de recuperação (base mensal)	Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m

8.3 - Destruição de Ativos na Nuvem

Resultado da Análise de risco		
Probabilidade: Média	**Impacto: Alto**	**Risco: Alto**

Descrição da ameaça:	Perda causada por destruição de ativos hospedados no provedor de nuvem. Embora a ameaça possa ser causada por ações acidentais, considera-se prevalentemente a realização de ações maliciosas no sentido de causar a referida destruição.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Rafael Angst - Gestor de Segurança da Informação (55) 99934-9920
Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Guillermo Elía - Analista de Infraestrutura (55) 99713-6568

Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Gestor de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Ativos de Suporte e Infraestrutura. “Inventário de Ativos.xlsx”
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Ambiente de Disaster Recovery (Azure EUA). Backup (Azure Recovery Services vaults)
Procedimentos:	1. Realizar restore do backup do ativo destruído (Azure Recovery Services Vaults). 2. Ativar o Plano de Recuperação de Desastre (DR) - “OP_0001_00 - Plano de Recuperação de Desastre de Data Center.docx” a. IT_0001_00 - Start de Banco de Dados no ambiente de DR.docx b. IT_0002_00 - Garantir o processo de conectividade no ambiente de DR.docx c. IT_0003_00 - Alterações de DNS Externo para Ambiente de DR.docx d. IT_0004_00 - Alterações em Servidores WEB para Ambiente de DR.docx e. IT_0005-00 _ Alterações em Servidores RDS para ambiente de DR.docx f. IT_0006-00 _ Alterações em Servidores APP para ambiente de DR.docx g. IT_0007-00 _ Alterações no Servidor de Arquivos para ambiente de DR.docx h. IT_0008_00 - Start de Banco de Dados no ambiente de DR - POSTGRESQL.docx i. IT_0010_00 - Validação de Sistemas para ambiente de DR.docx j. IT_0011_00 - Validação de Sistemas para ambiente de DR.docx k. IT_0012_00 - Alterações ConnectDirect.docx
Tempos objetivados de recuperação (base mensal)	Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min

	Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m

8.4 - Paralisação Parcial da Infraestrutura do Provedor de Nuvem

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Baixo**	**Risco: Muito baixo**
Obs. Com a utilização do provedor de nuvem Azure, leva-se em consideração a probabilidade de indisponibilidade com base no SLA disponibilizado pela Microsoft, conforme relatórios publicados em https://azure.microsoft.com/en-us/support/legal/sla/summary/. Os índices são por serviço e portanto foi considerado o menor, que no momento da elaboração deste documento era 99,9% de disponibilidade.		

Descrição da ameaça:	Risco relacionado à perda de funcionalidades ou disponibilidade causadas por mau funcionamento no provedor de nuvem. Considera-se parcial a possibilidade de tal paralisação, visto que o provedor de nuvem utilizado possui datacenters em mais de um local no mundo, não se considerando aqui a paralisação total de todos os datacenters do provedor Azure.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS (PCN)

Responsáveis pela execução do plano de recuperação:	Rafael Angst - Gestor de Segurança da Informação (55) 99934-9920
Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Guillermo Elía - Analista de Infraestrutura (55) 99713-6568
Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Gestor de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Ativos de Suporte e Infraestrutura. “Inventário de Ativos.xlsx”
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Os servidores/serviços possuem recursos de contingência. Ambiente de Disaster Recovery (Azure EUA).
Procedimentos:	1 - Ativar servidores/serviços de contingência. 2 - “OP_0001_00 - Plano de Recuperação de Desastre de Data Center.docx” levando em consideração os seguintes procedimentos: 23. IT_0001_00 - Start de Banco de Dados no ambiente de DR.docx 24. IT_0002_00 - Garantir o processo de conectividade no ambiente de DR.docx 25. IT_0003_00 - Alterações de DNS Externo para Ambiente de DR.docx 26. IT_0004_00 - Alterações em Servidores WEB para Ambiente de DR.docx 27. IT_0005-00 _ Alterações em Servidores RDS para ambiente de DR.docx 28. IT_0006-00 _ Alterações em Servidores APP para ambiente de DR.docx 29. IT_0007-00 _ Alterações no Servidor de Arquivos para ambiente de DR.docx 30. IT_0008_00 - Start de Banco de Dados no ambiente de DR - POSTGRESQL.docx 31. IT_0010_00 - Validação de Sistemas para ambiente de DR.docx 32. IT_0011_00 - Validação de Sistemas para ambiente de DR.docx 33. IT_0012_00 - Alterações ConnectDirect.docx
Tempos objetivados de recuperação (base mensal)	Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min

	Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m

8.5 - Destruição/Falha/Defeito de Equipamentos ou Mídias Relevantes

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Baixo**	**Risco: Muito baixo**

Descrição da ameaça:	Comprometimento de equipamentos locais (ex.: servidores, roteadores, switches,...) ou mídias tanto por ação maliciosa quanto por eventos naturais como surto elétrico.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo de Recursos Humanos: 98,80%
Dono do processo:	Laura Lorenset / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Guillermo Elía - Analista de Infraestrutura (55) 99713-6568
Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Jaime Zimmer - Analista de Infraestrutura (55) 99952-6191
Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Coordenador de Infraestrutura de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Servidor de Arquivos, Notebook, Desktop, mídias removíveis.
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Backup - ArcServe Backup. Equipamentos de Backup.
Procedimentos:	1. Realizar restore do backup do ativo (ArcServe Backup). 2. Substituir equipamento com defeito.
Tempos objetivados de recuperação (base mensal)	Processo de Recursos Humanos: 8h45m

8.6 - Interrupção de Suprimento de Energia

Resultado da Análise de risco		
Probabilidade: Alta	**Impacto: Baixo**	**Risco: Médio**

Descrição da ameaça:	Como os serviços prestados ao cliente estão hospedados na nuvem, a interrupção de suprimento não atinge os serviços oferecidos aos clientes, mas apenas os recursos mantidos na sede da instituição, o que representa, em suma, a possibilidade temporária dos colaboradores realizarem suas tarefas e/ou acessarem recursos de nuvem.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo de Recursos Humanos: 98,80% Obs: Os ativos hospedados na nuvem não têm sua continuidade afetada, ficando os serviços ainda disponíveis aos clientes. Porém, no intervalo da interrupção de energia e ativação do gerador, as equipes internas ficarão sem poder desempenhar suas atividades de trabalho.
Dono do processo:	Laura Lorenset / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Jaime Zimmer - Analista de Infraestrutura (55) 99952-6191
Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Guillermo Elía - Analista de Infraestrutura (55) 99713-6568
Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Coordenador de Infraestrutura de TI, Gestor de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Servidor de VPN, Servidor de Arquivos, Links de Comunicação (Internet).
Recursos de Infraestrutura de contingência para o funcionamento do processo:	MS SharePoint (Servidor de Arquivos), Conexão direta na Nuvem (VPN Azure). Nobreaks.

	Gerador de energia.
Procedimentos:	1. Ativar Gerador de energia.
Tempos objetivados de recuperação (base mensal)	Processo de Recursos Humanos: 8h45m

8-7 - Saturação de Sistema

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Baixo**	**Risco: Muito baixo**

Descrição da ameaça:	Dado um aumento das operações já existentes ou mesmo a inclusão de novas operações, pode ocorrer saturação de recursos na nuvem causando lentidão nas operações e, em casos extremos, parada de serviços. Não é considerado aqui ações maliciosas que, causando o mesmo efeito, constituiriam ataques de negação de serviço.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Rafael Angst - Gestor de Segurança da Informação (55) - 99934-9920

Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Jaime Zimmer - Analista de Infraestrutura (55) - 99952-6191
Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Ativos de Suporte e Infraestrutura. “Inventário de Ativos.xlsx”
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Ambiente de Disaster Recovery (Azure EUA).
Procedimentos:	**1. Ativar o Plano de Recuperação de Desastre (DR) - “OP_0001_00 - Plano de Recuperação de Desastre de Data Center.docx”** a. IT_0001_00 - Start de Banco de Dados no ambiente de DR.docx b. IT_0002_00 - Garantir o processo de conectividade no ambiente de DR.docx c. IT_0003_00 - Alterações de DNS Externo para Ambiente de DR.docx d. IT_0004_00 - Alterações em Servidores WEB para Ambiente de DR.docx e. IT_0005-00 _ Alterações em Servidores RDS para ambiente de DR.docx f. IT_0006-00 _ Alterações em Servidores APP para ambiente de DR.docx g. IT_0007-00 _ Alterações no Servidor de Arquivos para ambiente de DR.docx h. IT_0008_00 - Start de Banco de Dados no ambiente de DR - POSTGRESQL.docx i. IT_0010_00 - Validação de Sistemas para ambiente de DR.docx j. IT_0011_00 - Validação de Sistemas para ambiente de DR.docx k. IT_0012_00 - Alterações ConnectDirect.docx

Tempos objetivados de recuperação (base mensal)	Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m

8.8 - Indisponibilidade de Acesso à Internet na Sede da Instituição

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Baixo**	**Risco: Muito baixo**

Descrição da ameaça:	Interrupção do acesso à Internet na sede da empresa, impedindo a interação com os serviços disponíveis na nuvem.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Departamento Pessoal: 98,8% Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Departamento Pessoal: Carla Wagner / Fábio Groll Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Jaime Zimmer - Analista de Infraestrutura (55) - 99952-6191
Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Guillermo Elía - Analista de Infraestrutura (55) - 99713-6568)

Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Coordenador de Infraestrutura de TI, Gestor de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Link de Comunicação principal (Oi).
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Link de Comunicação de Contingência (Sygo).
Procedimentos:	1. Ativar Link de Comunicação de Contingência (automático). 2. Se ocorrer queda dos dois links, o acesso aos sistemas poderá ser realizado de qualquer local com internet, através de VPN com o Azure.
Tempos objetivados de recuperação (base mensal)	Processo Departamento Pessoal: 8h45m Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m

8.9 - Ataques de Ransonware

Resultado da Análise de risco		
Probabilidade: Alta	**Impacto: Alto**	**Risco: Crítico**

Descrição da ameaça:	Artefato de ransonware com acesso total à infraestrutura e aos dados da instituição, fruto de provável APT (Advanced Persistent Threat), que leva ao sequestro dos dados por meio de criptografia forte.
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo de Recursos Humanos: 98,8% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo de Recursos Humanos: Laura Lorenset / Fábio Groll Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Guillermo Elía - Analista de Infraestrutura (55) - 99713-6568

Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Jaime Zimmer - Analista de Infraestrutura (55) - 99952-6191
Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Gestor de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Ativos de Suporte e Infraestrutura. “Inventário de Ativos.xlsx”
Recursos de Infraestrutura de contingência para o funcionamento do processo.	Ambiente de Disaster Recovery (Azure EUA). Backup (Azure Recovery Services vaults)
Procedimentos:	1. Realizar restore do backup do ativo afetado (Azure Recovery Services Vaults). 2. Ativar o Plano de Recuperação de Desastre (DR). a. “OP_0001_00 - Plano de Recuperação de Desastre de Data Center.docx” b. IT_0001_00 - Start de Banco de Dados no ambiente de DR.docx c. IT_0002_00 - Garantir o processo de conectividade no ambiente de DR.docx d. IT_0003_00 - Alterações de DNS Externo para Ambiente de DR.docx e. IT_0004_00 - Alterações em Servidores WEB para Ambiente de DR.docx f. IT_0005-00 _ Alterações em Servidores RDS para ambiente de DR.docx g. IT_0006-00 _ Alterações em Servidores APP para ambiente de DR.docx h. IT_0007-00 _ Alterações no Servidor de Arquivos para ambiente de DR.docx i. IT_0008_00 - Start de Banco de Dados no ambiente de DR - POSTGRESQL.docx j. IT_0010_00 - Validação de Sistemas para ambiente de DR.docx k. IT_0011_00 - Validação de Sistemas para ambiente de DR.docx l. IT_0012_00 - Alterações ConnectDirect.docx

Processos de negócio afetados e índices de disponibilidade:	Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min Processo de Recursos Humanos: 8h45m Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m

8.10 - Perda da Sede Principal da Instituição

Resultado da Análise de risco		
Probabilidade: Baixa	**Impacto: Médio**	**Risco: Baixo**

Descrição da ameaça:	Situação gerada por qualquer evento que impeça a utilização da sede principal da instituição (ex. incêndio na própria ou em prédios vizinhos).
Ativos afetados pela ameaça:	Ativos relacionados aos processos de negócio conforme o Inventário de Ativos
Processos de negócio afetados e índices de disponibilidade:	Processo Departamento Pessoal: 98,8% Processo Comercial: 98,8% Processo de Cobrança: 98,8% Processo de Repasses: 98,8% Processo Administrativo Financeira: 99,4% Processo de Análise de Crédito: 98,8% Processamento de Dados: 99,4% Processo de Recursos Humanos: 98,8% Processo Cobrança Assessorias: 98,8% Processo Call Center: 98,8%
Dono do processo:	Processo Departamento Pessoal: Carla Wagner / Fábio Groll Processo Comercial: Ana Lugoch / Ademir Diel Processo de Cobrança: Airton Traesel / Moacir Engelmann Processo de Repasses: Elisiane Mombach / Paula Haubert Processo Administrativo Financeira: Paula Haubert / Fábio Von Groll Processo de Análise de Crédito: Fernando Ullmann / Joares Avrella Processamento de Dados: Leonardo Frantz / Wando Schneider Processo Cobrança Assessorias: Airton Traesel / Moacir Engelmann Processo Call Center: Carla Wagner / Fábio Groll
Responsáveis pela execução do plano de recuperação:	Jaime Zimmer - Analista de Infraestrutura (55) - 99952-6191
Responsáveis suplentes pela execução do plano de recuperação (com contatos inclusive):	Guillermo Elía - Analista de Infraestrutura (55) - 99713-6568)

Cargos ou pessoas a serem comunicados em caso da ativação:	Gestor de Segurança da Informação, Coordenador de Infraestrutura de TI, Gestor de TI.
Recursos de Infraestrutura utilizados para o funcionamento do processo:	Servidor de VPN, Servidor de Arquivos, Links de Comunicação (Internet).
Recursos de Infraestrutura de contingência para o funcionamento do processo.	MS SharePoint (Servidor de Arquivos), Conexão direta na Nuvem (VPN Azure).
Procedimentos:	1. Preparação da sede alternativa. 2. Utilizar os arquivos no MS SharePoint. 3. Realizar conexão de VPN direta no Provedor de Nuvem, para acesso aos ativos.
Tempos objetivados de recuperação (base mensal)	Processo Departamento Pessoal: 8h45m Processo Comercial: 8h45m Processo de Cobrança: 8h45m Processo de Repasses: 8h45m Processo Administrativo Financeira: 4h22min Processo de Análise de Crédito: 8h45m Processamento de Dados: 4h22min Processo de Recursos Humanos: 8h45m Processo Cobrança Assessorias: 8h45m Processo Call Center: 8h45m