CONFIDENCIAL (Não divulgar)

DEPARTAMENTO DE *CYBERSECURITY*

SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS (SGCN).

MODELO PARCIAL E ANONIMIZADO PARA FINS ACADÊMICOS

SÃO PAULO

20xx

HISTÓRICO DE REVISÕES

Tabela 1 - Revisões do plano.

Data	Versão	Descrição das modificações realizadas	Autor das modificações
14/05/2023	01	Modificação na tabela 3 (Mapeamento dos ativos)	Flávio Cunha.

CONTATOS PARA NOTIFICAÇÕES DE INCIDENTES

Tabela 2 - Contatos para notificações de incidentes.

Área	Cargo	Nome e sobrenome	E-mail	Celular
Tecnologia da Informação (TI)	Gerente			
Cybersecurity	Coordenador			
Parcerias externas contato principal	Gerente			
Parcerias externas suplente	Consultor			
CX – contato principal	Gerente			
CX - suplente	Consultora de atendimento			
Financeiro Contato principal	Gerente			
Financeiro Suplente	Consultora de finanças			
Desenvolvimento Contato principal	Gerente			
Desenvolvimento Suplente	Coordenadora de BAs			

INTRODUÇÃO

Escopo

Garantir que a empresa Confidencial esteja sempre preparada para atuar com eficiência diante de um incidente de disrupção. Permitindo assim, que as atividades de negócio que sustentam a entrega de produtos e serviços da companhia retornem a sua normalidade operacional dentro de critérios de tempo acordados previamente, a fim de que os impactos da indisponibilidade sejam os menores possíveis.

Objetivos do SGCN

- Servir como um guia para as equipes de continuidade de negócios da Confidencial.
- Fornecer procedimentos e recursos necessários para restabelecer as operações à sua normalidade após um evento de disrupção.
- Identificar clientes e fornecedores que devem ser notificados em casos de desastres e incidentes.
- Utilizar processos de gestão de riscos para identificar os ativos com maior e menor grau de risco para a companhia. Desta maneira, a recuperação dos ativos mais críticos para a organização podem ser priorizados.
- Ajudar a evitar confusão durante uma crise, com documentações atualizadas, testes e revisões periódicas dos procedimentos de recuperação.
- Identificar locais e fontes alternativas para hospedagem de infraestrutura, aplicações e serviços críticos.
- Começar priorizando a continuidade de negócios para os ativos mais críticos e com o tempo expandir o plano para áreas e ativos menos críticos.

Considerações importantes

Este plano foi elaborado para garantir que os pré-requisitos necessários para suportar um SGCN estejam presentes. Isto posto, esclarecemos que:

- Pessoas chaves (gestores de área) ou suplentes estarão disponíveis para apoio após um desastre ou evento de indisponibilidade.

- Este documento e todos os seus registros vitais devem estar armazenados em um local seguro fora das dependências da estrutura a ser recuperada após um evento de interrupção. Desta forma, poderá ser acessado imediatamento após o desastre.

- Um desastre nacional ou mundial como uma guerra está fora do escopo deste plano.

Ativos

Ativos são todos os elementos que possuem valor para uma organização. Alguns exemplos de ativos que podem ser encontrados em uma organização são os seguintes:

- **Ativos de infraestrutura**: Computadores, roteadores, *switches*.

- **Ativos de *Cloud***: Considera todo conjunto de aplicações e serviços de uma companhia alocados em algum provedor de *cloud*: *Amazon AWS, Google Cloud, Azure*, entre outros.

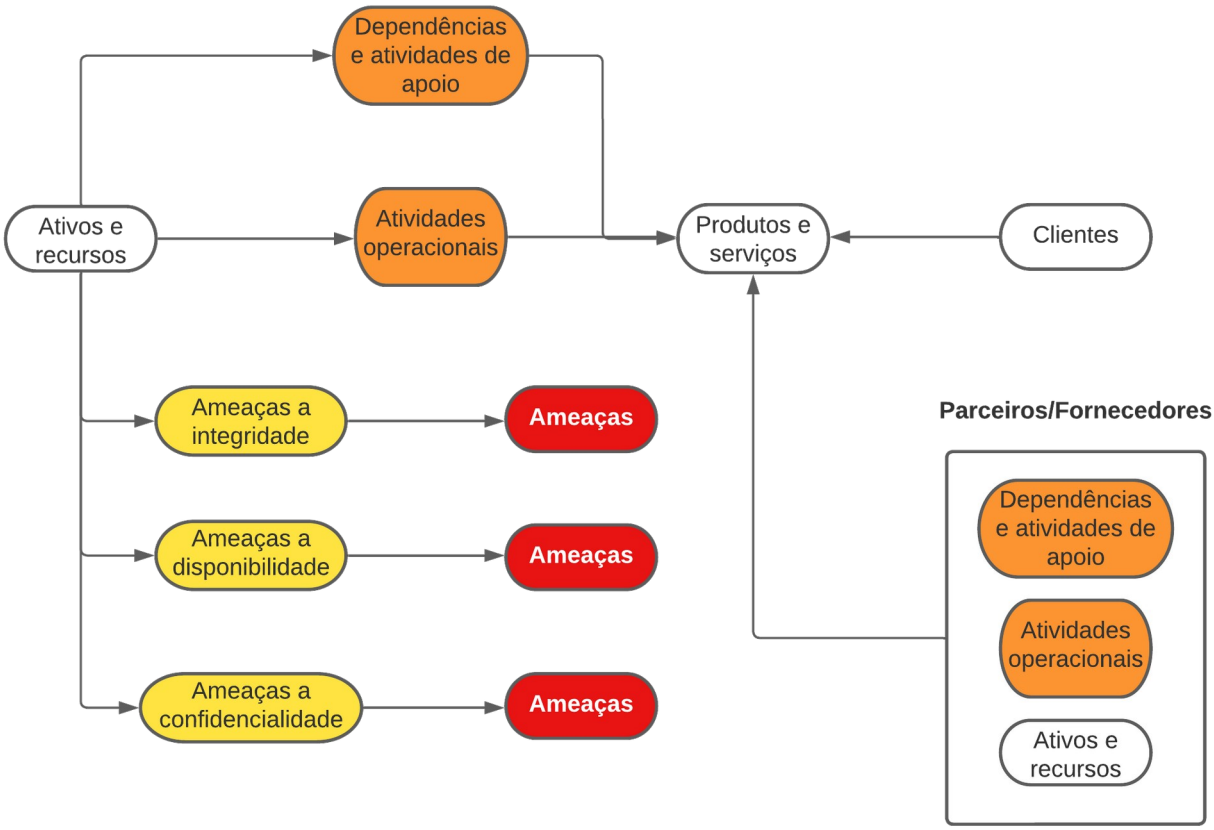
- **Ativos de Software**: Sistemas operacionais, aplicações, bibliotecas, Apps em geral.

- **Ativos de informações**: Folha de pagamento dos colaboradores, base de dados de clientes.

Este plano de continuidade de negócios considera todos os ativos que mantém o fornecimento dos produtos e serviços fornecidos pela organização. Os ativos constituem a base que mantém as atividades operacionais funcionando e as atividades operacionais

são responsáveis pela entrega dos produtos e serviços ofertados para os clientes. Portanto, o mapeamento adequado de todos os ativos e suas respectivas atividades operacionais é de fundamental importância para o estabelecimento de um SGCN eficiente. A figura 1, mostra a estrutura do SGCN da Confidencial.

Figura 1 - Estrutura do SGCN da Confidencial.



Uma vez que a estrutura do plano de continuidade de negócios seja definida o mapeamento dos ativos pode ser realizado. É importante ressaltar que para um SGCN somente os ativos que sustentam as atividades de negócio da companhia são considerados. A tabela 3, exibe os ativos definidos para este plano.

Tabela 3 - Mapeamento dos ativos Confidencial.

Ativo	Categoria do ativo	Atividades de negócio mantidas pelo ativo	Atividade operacionais que sustentam as atividades de negócio	Partes interessadas
confidencial.com.br	Aplicação web.	Site de pontos. Compra de pontos. Troca dos pontos por produtos e serviços.	Cluster Kubernets; APIs; Banco de dados Mysql (MDS); DNS; Backend: Microserviços; Frontend: OCC.	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.
confidencialshopping.com.br	Aplicação web.	Cashback. VIA (Outros E-commerces). Comissão.	Cluster Kubernets; APIs; Banco de dados Mysql (MDS); DNS; Backend: Microserviços; Frontend: OCC.	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.
App Android e IOS	Aplicação web.	Site de pontos. Compra de pontos. Troca dos pontos por produtos e serviços. Cashback e comissão.	Cluster Kubernets; APIs; Banco de dados Mysql (MDS); DNS; Backend: Microserviços; Frontend: OCC.	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.
Kong	API gateway,	API Gateway. Redirect de URL. Autenticação Basic Auth.	Cluster Kubernetes	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.

Ativo	Categoria do ativo	Atividades de negócio mantidas pelo ativo	Atividade operacionais que sustentam as atividades de negócio	Partes interessadas
Keycloak	Autenticação.	Autenticação dos usuários nas aplicações web: confidencial.com.br, confidencialshopping.com.br e nos App mobile (IOS e Android).	Cluster Kubernetes e banco de dados Mysql (MDS).	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.
Oracle Cloud (OCI)	Cloud	Sustentação de toda infraestrutura. Todo parque tecnológico. 100% na nuvem.	Provedor de cloud Oracle. A gestão é realizada pela Confidencial.	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.
Comarch CLM.	Parceiro. SAAS (*Software as a service*).	Gestor do sistema de pontos. (interno e Internet Pública).	A contingência é de responsabilidade do fornecedor. A garantia da Confidencial é o SLA (*Service Level Agreement*) do contrato.	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.

Ativo	Categoria do ativo	Atividades de negócio mantidas pelo ativo	Atividade operacionais que sustentam as atividades de negócio	Partes interessadas
Getnet	Parceiro	Gateway de pagamento.	A contingência é de responsabilidade do fornecedor. A garantia da Confidencial é o SLA (*Service Level Agreement*) do contrato.	Diretoria, Marketing, Novos negócios, Parcerias, CX/Atendimento, Fraude, Produtos, CRM, Finanças, TI, Dev.
Mysql	Banco de dados.			
Mongodb	Banco de dados.			

ANÁLISE E AVALIAÇÃO DE RISCOS

Dentro do contexto de segurança da informação, risco é a probabilidade de algum evento negativo ocorrer (indisponibilidades de serviços, invasões, roubo de informações, entre outros). Desastres naturais, desastres artificiais causados pelo homem, vulnerabilidades internas e externas em sistemas e infraestruturas são alguns exemplos que podem expor os ativos de uma companhia ao risco. Portanto, as organizações devem procurar se antecipar aos riscos e a adoção de medidas preventivas podem ajudar a mitigar ou diminuir os mesmos.

De acordo com a ABNT (27001:2006), o processo de análise de risco deve:

- Avaliar os ***impactos*** para o negócio da organização que podem resultar de falhas de segurança em ativos.

- Avaliar a ***probabilidade*** real da ocorrência das falhas de segurança.

- Estimar o ***grau*** ou nível do risco.

- Determinar a ***aceitação ou não do risco*** baseados em critérios para aceitação do risco previamente estabelecidos.

MENSURANDO O RISCO DOS ATIVOS

A matriz de risco é utilizada para calcular o grau de risco para um determinado ativo. Neste modelo, são aferidas a ***probabilidade*** de disrupção do ativo em determinado intervalo de tempo (normalmente um ano) e o ***impacto*** causado por esta indisponibilidade.

Tanto a probabilidade quanto o impacto são classificados dentro de uma escala de indisponibilidade que vai de 1 até 5. Onde, o valor 1 significa muito baixa e o valor 5 muito alta. A tabela 4, exibe esta classificação.

Tabela 4 - Nivel da propabilidade e do impacto da indisponibilidade em um ativo.

PROBABILIDADE/IMPACTO DA INDISPONIBILIDADE	
Valor	**Descrição**
1	Muito baixa
2	Baixa
3	Média
4	Alta
5	Muito alta

CÁLCULO DA PROPABILIDADE DE INDISPONIBILIDADE PARA OS ATIVOS DA CONFIDENCIAL

A meta de SLA (*Service Level Agreement*) definida pela gestão da companhia para os ativos foi utilizada a fim de determinar a probabilidade de indisponibilidade dos mesmos.

O SLA se refere ao nível de serviço acordado entre duas partes. Por exemplo: um cliente e um prestador de serviço. Normalmente, dentro do contexto de um plano de continuidade de negócios o SLA dos ativos é acordado entre as áreas responsáveis pelo SGCN e a área de negócios da organização e tem a ver com a disponibilidade do serviço ou ativo dentro de um determinado intervalo de tempo (normalmente, 1 ano).

A meta de SLA acordada para todos os ativos da companhia é de 99,5%. O que equivale a um tempo de indisponibilidade de 43,8 horas por ano. Desta forma, consideramos que os ativos que possuem valores de SLA acima da meta possuem probabilidades baixas ou muito baixas de indisponibilidade, enquanto os ativos que possuem valores de SLA abaixo da meta possuem probabilidade de indisponibilidade média, alta ou muito alta.

A tabela 5, mostra a probabilidade de indisponibilidade com os respectivos valores de SLA.

Tabela 5 - Faixas de SLA e probabilidade de indisponibilidade em um ano.

SLA em %	Probabilidade de indisponibilidade	Horas de indisponibilidade por ano.
99,9	Muito baixa	8,76
99,8	Muito baixa	17,52
99,7	Baixa	19,5
99,6	Baixa	35,4
99,5	Meta definida	43,8 (1,8 dias)
99,4	Média	52,56
99,3	Média	61,32
99,2	Alta	70,08
99,1	Alta	78,84
99,0	Muito alta	87,6 (3 dias e meio)
98,9	Muito alta	96,36 (4 dias)

CÁLCULO DO IMPACTO DA INDISPONIBILIDADE PARA OS ATIVOS DA CONFIDENCIAL

Para determinar o nível de impacto causado pela indisponibilidade dos ativos da Confidencial, utilizamos quatro critérios de classificação (financeiro, reputacional, operacional e legal e regulamentar). Onde a média deste critérios determina o valor de impacto que será atribuído na matriz de risco, conforme mostra a tabela 6.

Tabela 6 - Tipos de impacto causados pela indisponibilidade de produtos e serviços.

TIPOS DE IMPACTO	
Financeiro	Perdas com multas, penalidades, perda de lucro.
Reputacional	Danos à marca. Opinião negativa.
Operacional	Interrupções no fluxo de operações do negócio.
Legal e regulamentar	Responsabilidade por litígios, cancelamento de licenças para negociação.

Por exemplo, conforme descrito na tabela 4, considera-se que um determinado ativo tenha os seguintes valores de impactos: Financeiro: 4 (Alto), Reputacional: 3 (Médio), Operacional: 5 (Muito alto) e legal e regulamentar: 1 (muito baixo). Logo, calculando-se a média temos: 4 + 3 + 5 + 1 / 4 = 3,25. Arredondando para um valor inteiro, temos 3. Portanto, o impacto da indisponibilidade deste ativo é 3 (médio).

GRAU DE RISCO DOS ATIVOS

Após o estabelecimento de valores para o impacto e para a probabilidade de indisponibilidade dos ativos, pode-se calcular o grau de risco.

O grau de risco é o valor usado como referência para mensurar os riscos que um determinado ativo apresenta. Valores altos significam alta exposição ao risco, enquanto valores baixos indicam baixa exposição ao risco.

O grau de risco dos ativos é calculado multiplicando-se a probabilidade pelo impacto.

Grau de risco = Probabilidade x Impacto

Exemplo: utilize a matriz de risco da tabela 7 para calcular o grau de risco de um ativo que possua probabilidade 3 e impacto 5.

Resposta: 3 x 5 = 15. **Logo, o ativo possui grau de risco 15**. Ao consultar os valores da tabela 8, verifica-se que o ativo possui um grau de risco alto.

Tabela 7 - Matriz de risco dos ativos.

IMPACTO	**GRAU DE RISCO DOS ATIVOS**				
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
PROBABILIDADE	1	2	3	4	5

Tabela 8 - Valores para o grau de risco.

VALORES PARA O GRAU DE RISCO	
Muito baixo	1 a 2
Baixo	3 a 5
Médio	6 a 10
Alto	12 a 16
Muito alto	20 a 25

A partir deste ponto, os outros tópicos do SGCN são desenvolvidos.

MAPEAMENTO DE RISCO PARA OS ATIVOS

BIA (*Business Impact Analysis*)

RTO (*Recovery Time Objective*) e RPO (*Recovery Point Objective*)

Priorização de ativos para contingência

Acões dentro de um contexto de risco

Apêndice A – Procedimentos de DR (*Disaster Recovery*) para as aplicações.

Procedimento do PCN

1. Declarar e ativar a contingência.
2. Acionar a equipe de resposta.
3. Executar o plano de contingência.
4. Preparar o relatório de contingência
5. Notificar o fim da contingência.