1. Política de Backup e Restauração

Este documento estabelece políticas de cópia de segurança (backups), armazenamento e restauração de dados digitais presentes nos servidores dessa organização.

Os proprietários dos dados devem ter ciência dos termos deste documento e dos tempos de retenção a serem praticados para cada tipo de informação e o corpo técnico deve assegurar as ações necessárias para que estas sejam cumpridas.

1.2 – Matriz de Responsabilidade

O administrador de backup é responsável por conhecer a política de backup, identificar acordos e instruções normativas que se relacionem com esta, planejar e executar operações de backup para todos os servidores e sistemas da Intelitrader Tecnologia, preferencialmente depois do horário do expediente a fim de não obter nenhum impacto na operação durante o tempo ativo dos colaboradores. Ele é responsável também pelo monitoramento, correta execução dos backups, ajustes, reexecução dos backups em caso de falhas e aderência a todos os requisitos operacionais requeridos, tais como janela de execução, procedimentos específicos de backup de determinada aplicação, dentre outros.

O administrador de restauração é responsável por receber e processar demandas eventuais de restauração de dados, por realizar testes de restauração periódicos de acordo com o cronograma que foi definido junto ao CSI.

É feito o backup dos dados sensíveis existentes nos sistemas desenvolvidos pela Intelitrader. Todos estes são focados em suprir as demandas dos clientes.

Sistemas internos, de comunicação, gestão e etc., são adquiridos de fornecedores externos onde estes são responsáveis pela rotina do backup.

1.3 - Sistemas Afetados

É feito o backup dos dados sensíveis existentes nos sistemas desenvolvidos pela Intelitrader. Todos estes são focados em suprir as demandas dos clientes.

Sistemas internos, de comunicação, gestão e etc., são adquiridos de fornecedores externos onde estes são responsáveis pela rotina do backup.

1.4 – Periodicidade do Backup e tempo de Retenção

Os seguintes dados e aplicação serão copiadas de acordo com a Estratégia de Rotação GFS Clássico, em backups diários com método de backup diferenciais, mais os semanais, mensais e anuais (históricos) como modo backup full, com a retenção mínima de 7,31, 365 dias e 5 anos, respectivamente seguindo o Escopo relacionado neste documento.

Segue abaixo o nosso modelo GFS definido:

DOM	SEG	TER	QUA	QUI	SEX	SAB
Nenhum	Dif*	Dif*	Dif*	Dif*	Dif*	Full

*** Dif – Backup Diferencial * Full – Backup Completo**

Modelo do Cronograma de Backup do Mês Inteiro:

DOM	SEG	TER	QUA	QUI	SEX	SAB
1	2	3	4	5	6	7
Nenhum	Dif	Dif	Dif	Dif	Dif	F-Mensal
8	9	10	11	12	13	14
Nenhum	Dif	Dif	Dif	Dif	Dif	F-Semana
15	16	17	18	19	20	21
Nenhum	Dif	Dif	Dif	Dif	Dif	F-Semana
22	23	24	25	26	27	28
Nenhum	Dif	Dif	Dif	Dif	Dif	F-Semana
29	30	31	1	2	3	4
Nenhum	Dif	Dif	Dif	Dif	Dif	F-Mensal

*** Dif – Backup Diferencial**

*** F-Mensal – Backup Full Mensal**

*** F-Semana – Backup Full Semanal**

1.5 – Gestão Simplificada de Riscos

Para a finalidade deste documento, a seguinte notação é utilizada para o registro de riscos levantados

Modelo
Risco#:[Fato gerado do risco]

Impacto:[baixo,médio,alto]

Tipo de Risco (C,D,I): [Confidencialidade, Disponibilidade, Integridade]

Ação: [procedimentos para mitigação ou eventual aceitação de risco]

Durante o ciclo atual de gestão de riscos, estes foram os levantados e classificados para fins de mitigação.

Risco 01: Crescimento exagerado da demanda de espaço de armazenamento para backup.

Impacto: Médio

Tipo do Risco: (D) Disponibilidade

Ação: Comprar mais HDs para armazenamento e/ou solicitar o aumento de espaço em nuvem

Risco 02: Infecção por Ransomware no Backup Local.

Impacto: Alto

Tipo do Risco: (C,D,I) Confidencialidade, Disponibilidade, Integridade

Ação: Verificar se o servidor está com antivírus instalado e ativado, mitigar a causa da infecção, formatar a unidade de disco local e restaurar o banco de backup através do backup em nuvem.