**Cenário de testes para Plano de Continuidade de negócios.**

Este documento visa estabelecer as diretrizes para condução dos testes em conformidade com o item 13 do “Plano de Continuidade de Negócios” desta instituição.

# Cenários a serem verificados

Durante o exercício devem ser efetuados os seguintes cenários de testes:

|  |  |  |  |
| --- | --- | --- | --- |
| **Código** | **Descrição** | **Periodicidade** | **Área Resp.** |
| 1 | Criptografia em toda a extensão que possuem alguma exposição com a rede de internet. | Anual | TI |
| 2 | Rotacionamento de senhas e credenciais de acesso dos usuários a seus sistemas e infraestrutura. | Semestral | TI |
| 3 | Teste de stress sobre a camada de Internet Banking. | Trimestral | TI |
| 4 | Teste de integridade de dados | Semestral | TI |
| 5 | Teste de recuperação de desastre | Anual | TI |

# Procedimentos e controles adotados aos fornecedores de armazenamento e processamento de dados

|  |  |
| --- | --- |
| **Item** | **Descrição** |
| 1 | Formalização de Termo de Confidencialidade com os fornecedores da instituição. |
| 2 | Toda a troca de informações deve ocorrer em ambiente corporativo, utilizando ferramentas de comunicação da instituição, e, quando não possível, esclarecer em documento específico qual a ferramenta utilizada e suas limitações quanto a segurança, a ser assinado pela instituição e pelo prestador de serviço. |
| 3 | Exigência que o prestador envie a instituição evidência de testes de recuperação de desastre em seu ambiente e/ou verificação própria em casos que a administração assim determine. |
| 4 | Teste de integridade com amostragem de dados entre o banco de dados em produção e o último backup disponibilizado. |

# Forma de classificação de dados quanto a sua relevância.

A classificação dos dados e das informações quanto à relevância devem seguir a escala a seguir:

|  |  |  |
| --- | --- | --- |
| **Tipo** | **Descrição** | **Grau de Incidente** |
| INFORMAÇÃO PÚBLICA | A informação deve ser classificada como pública quando ela puder ser divulgada a todos, isto é, funcionários, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio. Apesar de uma informação pública não precisar de nenhum tipo de proteção quanto à questão do sigilo, é conveniente que usuário nenhum tenha acesso a ela, a menos que precise de tal informação para o desempenho de suas atividades. | 1 |
| INFORMAÇÃO INTERNA | A informação deve ser classificada como interna quando não for desejável que ela se torne conhecida por pessoas de fora da organização. Contudo, caso haja vazamento e ela se torne de conhecimento público, é característica da informação classificada como interna a impossibilidade da ocorrência de um grande prejuízo à organização.Como são informações relevantes para o funcionamento dos negócios, precisam principalmente ter sua integridade protegida. | 2 |
| INFORMAÇÃO CONFIDENCIAL | A informação deve ser classificada como confidencial quando sua exposição fora do ambiente da organização possa acarretar em perdas financeiras, de imagem, de competitividade etc.Para proteção de uma informação confidencial, se faz necessário, além de controles de acesso, controles que garantam sua integridade, pois são informações importantíssimas para as atividades do negócio. Informações confidenciais, por exemplo, jamais podem ser transmitidas via Internet sem o uso de criptografia e, quando descartadas, devem ser tomadas as providências cabíveis para que a informação seja de fato destruída, sem chance de recuperação. | 3 |
| INFORMAÇÃO RESTRITA | A informação deve ser classificada como restrita quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos ao negócio. Logo, a informação restrita precisa ser protegida contra acessos internos e externos. São ainda mais importantes que as informações confidenciais e por isso devem receber um grau de proteção ainda mais elevado.Só devem ter acesso a informações restritas pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado. | 4 |

# Parâmetros de Relevância de Incidente

|  |  |  |
| --- | --- | --- |
| **Grau** | **Ação Imediata** | **Responsável** |
| 1 | Comunicação do vazamento da informação ao órgão de auditoria interna e controladoria interna para fins de registro e melhoria dos procedimentos internos, com foco no procedimento ao qual tenha originado o vazamento. | Controles Internos |
| 2 | Comunicação do vazamento da informação ao órgão de auditoria interna e controladoria interna para fins de registro e melhoria dos procedimentos internos, com foco no procedimento ao qual tenha originado o vazamento.Comunicação ao Conselho de Administração do fato ocorrido após levantamentos evidenciados pela controladoria da instituição para registro em ATA do fato e do plano de ação a ser adotado para evitar este tipo de ocorrência. | Controles Internos e Conselho de Administração |
| 3 | Comunicação do vazamento da informação ao órgão de auditoria interna e controladoria interna para fins de registro e melhoria dos procedimentos internos, com foco no procedimento ao qual tenha originado o vazamento.Comunicação ao Conselho de Administração do fato ocorrido após levantamentos evidenciados pela controladoria da instituição para registro em ATA do fato e do plano de ação a ser adotado para evitar este tipo de ocorrência.  | Controles Internos e Conselho de Administração |
| 4 | Comunicação do vazamento da informação ao órgão de auditoria interna e controladoria interna para fins de registro e melhoria dos procedimentos internos, com foco no procedimento ao qual tenha originado o vazamento.Comunicação ao Conselho de Administração do fato ocorrido após levantamentos evidenciados pela controladoria da instituição para registro em ATA do fato e do plano de ação a ser adotado para evitar este tipo de ocorrência. Também deverá o Conselho de Administração, deliberar sobre a comunicação de eventual vazamento de dados ao mercado na forma da lei vigente. | Controles Internos e Conselho de Administração |