Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Registro de LOGs

Objetivo

Estabelecer procedimentos de manutenção de informações e registros em todos os sistemas utilizados pela Instituição, incluindo medidas para o controle e monitoramento das Políticas, normas e regulamentos da Instituição, nos termos do art. 37 da LGPD.

Visão geral

Os registros de todas as ações realizadas nas plataformas e sistemas da Instituição são importantes para garantir o rastreio de quaisquer condutas danosas ou para fins de auditoria. A LGPD dispõe, em seu art. 37, que: “O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse”. Portanto, para os fins desta Política, poderão ser rastreados e monitorados (i) os acessos individuais do usuário a sistemas que contêm toda e qualquer tipo de informação da Instituição; (ii) os acessos individuais do usuário com credenciais de acesso nos sistemas da Instituição; (iii) os acessos e pausas dos registros de auditoria; (iv) tentativas e falhas de acesso nos sistemas da Instituição; (v) as alterações, adições ou exclusões realizadas em contas com credenciais e sem credenciais.

EMBRASI

Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

1. Diretrizes de Manutenção de Registros

Todos os sistemas de controle e tratamento de informações confidenciais, controle de conexões de rede, controle de acessos e controle de procedimentos de autenticação e autorização devem registrar as informações de:

- Quais atividade foram realizadas;
- Quem realizou a atividade, incluindo em que sistema foi realizada a atividade;
- Quando a atividade foi realizada;
- Determinar se a atividade realizada foi bem sucedida ou não;
- Sistemas e ativos tecnológicos envolvidos.

Para fins de controle e auditoria, seguindo as diretrizes da Política de Auditoria Interna (PAI), o Responsável pela Segurança da Informação deve implementar uma infraestrutura de registro adequada a abranger todos os dispositivos, sistemas e aplicativos utilizados pela Instituição.

Deste modo, o software de análise de integridade e detecção de alterações da Instituição deve revisar periodicamente os registros e emitir alertas se os dados de registro forem alterados.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

2. Procedimentos de Registro

Os registros devem necessariamente monitorar as seguintes atividades:

- Criação, leitura, modificação ou exclusão de Informações Confidenciais;
- Iniciação ou criação de uma nova conexão de rede;
- Autenticação do acesso ao usuário e posterior autorização de segurança;
- Concessão, modificação ou revogação dos direitos de acesso para usuários ou grupos;
- Modificação de privilégios de usuário;
- Modificação de permissões de sistemas, ativos tecnológicos e serviços;
- Alteração de senhas de usuário;
- Configurações de sistemas, redes ou serviços para alterações de manutenção e segurança, incluindo as atualizações dos softwares instalados;
- Alterações do status de inicialização, de desligamento ou de reinicialização de sistemas;
- Falhas de sistema e aplicações, causadas pela utilização limite de recursos informáticos (CPU, memória, largura de banda de rede, espaço em disco, dentre outros);
- Falha nos serviços de rede;
- Falha de sistemas de hardware;
- Detecção de atividades suspeitas e maliciosas por sistemas antivírus ou de firewall.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

3. Procedimentos de Revisão de Registro

Cada integrante ou equipe da Instituição é responsável por revisar e monitorar os registros de sistemas sob seu controle. Os registros devem ser revisados periodicamente pelo Responsável pela Segurança da Informação.

A frequência de revisão também deve ser determinada pelo Responsável pela Segurança da Informação, de acordo com a sensibilidade das informações armazenadas.

Os procedimentos de revisão devem verificar se:

- Os eventos estão sendo devidamente classificados;
- Não estão havendo atrasos de desempenho;
- O registro relacionado à conformidade não possa ser ignorado pelo usuário;
- O acesso aos arquivos de registro está sendo devidamente restrito a quem não possui as credenciais necessárias;
- Há possibilidade de auxiliar nas investigações internas da Instituição.

4. Elementos de Registro

As entradas de registro podem conter uma série de informações, dentre as quais:

- Identificação do ativo informático;
- Data e hora do registro;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Identificação do aplicativo (incluindo o nome e a versão);
- Identificação do evento de origem do registro (por exemplo, URL de ponto de entrada, página, formulário);
- Localização do código (por exemplo: módulo, sub-rotina);
- Ação de início do usuário (por exemplo: ID do usuário);
- Tipo de evento;
- Status do resultado (por exemplo: sucesso, falha, adiamento);
- Recurso (por exemplo: identidade ou nome dos dados afetados, componentes);
- Localização (por exemplo: endereço IP ou localização geográfica);
- Gravidade do evento (por exemplo: emergência, alerta, erro fatal, aviso, somente informações);
- Outros (por exemplo: parâmetros, informações de depuração, mensagem de erro do sistema);

5. Formatação e Armazenamento de Registros

O sistema deve garantir a formatação e o armazenamento dos registros para garantir a integridade e a legibilidade dos relatórios gerados para fins de auditoria. Assim, para a adequação dos registros com a Política de Auditoria Interna (PAI), deve-se centralizar as entradas de registro dos bancos de dados da Instituição em um único servidor, respeitando-se as diretrizes da Política de Backup (PBAC), com a respectiva

padronização dos registros e também dos protocolos de envio a um servidor centralizado.

6. Gerenciamento de Ameaças de Segurança da Informação

O sistema de registros é a principal ferramenta utilizada pela Instituição para detectar e investigar atividades não autorizadas e para solucionar eventuais problemas em seus sistemas. Portanto, devem ser desenvolvidos procedimentos para proteger e mitigar ameaças de segurança aos registros da Instituição, tais como:

- Limitação dos usuários aptos a desativar, danificar ou contornar mecanismos de acesso aos registros e trilhas de auditoria;
- Proteção do conteúdo dos registros do sistema contra acessos, modificações ou exclusões não autorizados;
- Limitação do acesso remoto aos sistemas de registro àquelas circunstâncias extremas ou emergenciais. Deste modo, qualquer acesso a estes sistemas deve ser autorizado pelo Responsável pela Segurança da Informação e o uso de ferramentas que contornem os controles de segurança deve ser devidamente documentado;
- Limitação das alterações em todas as Políticas Gerais, mas especialmente na Política de Auditoria Interna (PAI), a fim de impedir alterações indevidas e não autorizadas.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

7. Responsabilidades no Gerenciamento de Registros

O Responsável pela Segurança da Informação deve:

- Separar os deveres entre as funções de operação e as funções de monitoramento incluídas nesta Política;
- Aprovar os tipos de registros e relatórios a serem gerados, revisando atividades e procedimentos a serem realizados;
- Observar os procedimentos específicos de auditoria contidos na Política de Auditoria Interna;
- Estabelecer procedimentos específicos para tentativas de login malsucedidas, discrepâncias em relatórios e procedimentos utilizados para monitorar tentativas de login;
- Revisar periodicamente os registros de auditoria, relatórios de acesso e incidentes de segurança;
- Estabelecer procedimentos para garantir que os controles de auditoria atendam aos requisitos de segurança, especialmente no tocante àquelas atividades envolvendo Informações Confidenciais da Instituição;
- Garantir que os arquivos para fins de auditoria estejam prontamente disponíveis, de acordo com Política de Backup (PBAC).