Política de Segurança da Informação

SUMÁRIO

1. APRESENTAÇÃO

Para manter a continuidade do negócio do Grupo Disbral, em sua missão como empresa provedora de soluções tecnológicas com foco na gestão pública municipal, é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de perdas por erro humano, ataques externos, catástrofes naturais ou outras ameaças. No sentido de assegurar a proteção dos dados eletrônicos desta Empresa, o presente documento apresenta a política de backup e restauração, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

2. OBJETIVO

Definir o tratamento dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente de tecnologia do Grupo Disbral.

As orientações aqui apresentadas são os princípios fundamentais para nortear a definição de procedimentos, instruções normativas e instruções de trabalho alinhados à segurança da informação exigida pela companhia, bem como a implementação de controles e processos para seu atendimento.

3. ESCOPO

Este documento é aplicado ao escopo interno do Sistema de Gerenciamento de Segurança da Informação (ISMS) e a todas as atividades de processamento de dados do negócio do Grupo Disbral.

4. ABRANGÊNCIA

Este documento aplica-se a todos os funcionários, clientes e fornecedores de serviços do Grupo Disbral.

Esta Política define não apenas os requisitos de segurança lógica, mas, também, os de segurança física nos ambientes computacional e convencional.

5. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27001:2013, ANEXO A.
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

6. USO ACEITÁVEL DE ATIVOS DE INFORMAÇÃO

6.1. Glossário

Para os efeitos desta política aplicam-se os termos do disposto neste documento, e subsidiariamente os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

TERMO	DEFINIÇÕES
Ameaça	Agentes ou condições causadoras de incidentes de segurança. Exploram as vulnerabilidades em sistemas e serviços.
Ativos de informação	No contexto desta política, o termo ativo de informação é aplicado para sistemas de informação e outras informações/equipamentos incluindo, informações em papéis, celulares, computadores portáteis, mídias de armazenamento etc.
Autenticidade	Garantia de que o dado ou informação são verdadeiros.
Backup	Processo de salvaguarda de dados com o objetivo de amenizar os efeitos decorrentes da perda dos originais.
Banco de Dados	Software usado para gerenciar a Base de Dados da empresa.
Classificação da Informação	Processo de identificar e definir níveis critérios de proteção adequados para as informações de forma a garantir sua confidencialidade, integridade e disponibilidade.
Confidencialidade	Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
Controle de Acesso	Restrições de acesso a um ativo do Grupo Disbral.
Comitê Gestor de Segurança Informação (CGSI)	Instância responsável pela elaboração e revisão periódica da Política de Segurança da Informação e normas relacionadas. Auxilia os departamentos da empresa na implementação das ações de segurança da informação.
Controle de Segurança	Práticas de gestão de risco (políticas, normas, procedimentos ou mecanismos) que podem proteger os ativos contra ameaças, reduzir ou eliminar vulnerabilidades e limitar o impacto de um incidente de segurança.
Direito de Acesso	Privilégio associado a um usuário para ter acesso a um ativo.
Dado Pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado Pessoal Sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Disponibilidade	Propriedade de que a informação esteja acessível e utilizável quando demandada.
Gestor da Informação	Pessoa responsável pela autorização de acesso, validação de uso e definição dos demais controles sobre a informação. Cada serviço deverá ter o seu Gestor que será indicado formalmente pela diretoria.
Gestão de risco	Atividade contínua de identificação, análise, tratamento, aceitação e comunicação de riscos.
Incidente de Segurança	Qualquer evento que resulte no descumprimento da Política de Segurança da Informação e que possa representar uma ameaça.

Integridade	Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
Log	Registro de eventos ocorridos nos sistemas computacionais. Deve conter: data e hora da atividade, identificação do usuário, do computador e dos procedimentos executados.
Monitoramento	Acompanhamento de eventuais ameaças, incidentes de segurança ou quaisquer descumprimentos às diretrizes presentes nas Políticas, Normas ou Procedimentos de Segurança da Informação.
Privacidade	Condição daquilo que é privado, pessoal, íntimo.
Proteção de Dados pessoais	É um meio de adoção de adoção de medidas necessárias para garantir a privacidade.
Plano de Continuidade de Negócio (PCN)	Documento que define o processo de gestão da capacidade do Grupo Disbral manter um nível de funcionamento adequado até o retorno à situação normal, após a ocorrência de incidentes e interrupções de sistemas críticos.
Plano de Resposta a Incidentes	Documento que estabelece ações que visam minimizar o impacto de um incidente e permitir o restabelecimento dos serviços o mais rápido possível.
Regimento Interno	Define as atribuições de todos os cargos e departamentos do Grupo Disbral.
Regulamento Disciplinar	Determina critérios disciplinares dos colaboradores do Grupo Disbral, divulgando conceitos, deveres e proibições, visando o funcionamento harmônico do comportamento funcional e estabelecendo competências para adoção de eventuais penas disciplinares.
Risco	Probabilidade de uma determinada ameaça se concretizar.
Segurança da Informação	Conjunto de medidas voltadas a salvaguardar dados e informações sigilosos gerados, armazenados e processados por intermédio da informática, bem como a própria integridade dos sistemas desenvolvidos e utilizados pela empresa.
Sistema de Informação	Inclui todos servidores e desktop, infraestrutura de redes, sistemas e aplicações, dados, e outros componentes que sejam de propriedade da DISBRAL ou que estão sob sua responsabilidade. O uso de um sistema de informação também inclui o uso de todos os serviços internos ou externos, tais como acesso à Internet, e-mail corporativo etc.
Titular do Dado	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
Vulnerabilidade	Fragilidades associadas aos ativos que os tornam susceptíveis às ameaças.

6.2. Uso aceitável

Ativos de informação podem ser usados somente para atividades ligadas ao negócio do Grupo Disbral.

6.3. Responsabilidade para os ativos

Cada ativo de informação deve ter um responsável designado pela Direção no Inventário de Ativos. O responsável pelo ativo deve definir as questões de confidencialidade, integridade e disponibilidade.

6.4. Atividades proibidas

É proibido usar ativos de informação de maneira que ocupe desnecessariamente a capacidade, enfraqueça o desempenho do sistema de informação ou represente uma ameaça à segurança ao Grupo Disbral. Também é proibido:

- Fazer download de arquivos de imagem ou vídeo que não tenham uma finalidade comercial, enviar mensagens de corrente por e-mail, jogar jogos etc.
- Instalar o software em um computador local sem permissão explícita da equipe de TI.
- Usar aplicativos Java, controles Active X e outros códigos móveis, exceto quando autorizado pelo analista de infraestrutura.
- Usar ferramentas criptográficas (criptografia) em um computador local, exceto nos casos especificados pela equipe de TI.
- Copiar ou instalar programas de mídias externa.
- Instalar ou usar dispositivos periféricos, como modems externos, cartões de memória ou outros dispositivos para armazenar e ler dados (por exemplo, pen drives) sem permissão explícita da equipe de TI;

6.5. Remover ativos para fora das instalações do Grupo Disbral

Equipamentos, informações ou software, independentemente de sua forma ou meio de armazenamento, não podem ser retirados do local sem a permissão prévia por escrito da direção do Grupo Disbral.

Enquanto esses ativos estiverem fora da organização, eles devem ser controlados pela pessoa que recebeu permissão para retirada.

6.6. Devolução de ativos após a rescisão do contrato

Após a rescisão de um contrato de trabalho ou outro contrato com base no qual vários equipamentos, software ou informações em formato eletrônico ou em papel são usados, o usuário deve devolver todos os ativos de informações para equipe de TI.

6.7. Procedimento de backup

As Informações relevantes devem ser armazenadas de forma redundante para garantir a disponibilidade e restauração de arquivos digitais de computadores e sistemas corporativos de acordo com as normas vigentes.

6.7.1 Objetivo

Assegurar a proteção, integridade, disponibilidade e recuperação das informações institucionais por meio da execução de rotinas de backup locais e em nuvem.

6.7.2 Escopo

Aplicável à equipe de TI (analistas e encarregados), responsável pela instalação, configuração, monitoramento e validação dos processos de backup.

6.7.3 Diretrizes

6.7.3.1 Modelos de Backup

Backup em nuvem (Acronis/Algar Cloud):

Backup total: realizado no **primeiro dia de cada mês às 22h40**.

Backup incremental: realizado **diariamente às 22h40**.

Backup local (Proxmox e Windows Server):
Backup total diário, armazenado em **storages locais** dedicados.

6.7.3.2 Processo e Monitoramento

Backups em nuvem são enviados automaticamente ao portal Algar e monitorados pelo **painel de controle online**.
Backups locais são geridos pelos **agendadores do Proxmox e Windows Server**, com acesso via **painel de administração interno**.
A equipe de TI deve realizar **verificação diária** para confirmar execução, integridade e armazenamento adequado dos arquivos.
A equipe de TI não efetuará backup de arquivos armazenados localmente nas estações de trabalho, portanto, para armazenamento de arquivos deve-se utilizar os diretórios da rede.

6.7.3.3 Notificação de Falhas

No backup em nuvem, falhas geram alertas automáticos enviados para o e-mail institucional da TI.
No backup local, inconsistências devem ser acompanhadas no painel de gestão e reportadas internamente.

6.7.3.4 Armazenamento e Segurança

Nuvem: utilização de repositório seguro Algar Cloud, com autenticação e credenciais controladas.
Local: utilização de storages internos, acessíveis somente a administradores autorizados.
Em ambos os casos, a integridade dos dados deve ser validada periodicamente.

6.7.3.5 Responsabilidades

Equipe de TI: executar, monitorar, validar e documentar rotinas de backup.
Gestores: prover infraestrutura, supervisionar conformidade e revisar periodicamente a política.

6.7.4 Revisão

Esta política deve ser revisada periodicamente, pelo menos a cada quatro anos, ou sempre que houver mudanças significativas em sistemas, infraestrutura ou ferramentas utilizadas.

6.8. Proteção de antivírus

O antivírus ***BitDefender*** deve ser instalado em cada computador com atualizações automáticas ativadas.

6.9. Autorizações para uso do sistema de informação

Os usuários só podem acessar os ativos de informação para os quais foram explicitamente autorizados pelo proprietário do ativo.

Os usuários podem usar o sistema de informação apenas para os fins para os quais foram autorizados, ou seja, para os quais foram concedidos direitos de acesso.

Os usuários não devem participar de atividades que possam ser utilizadas para contornar os controles de segurança do sistema de informação.

6.10. Responsabilidade pelas credenciais de acesso

O usuário não deve, direta ou indiretamente, permitir que outra pessoa utilize suas credenciais de acesso, como nome de usuário e senha, nem deve utilizar as credenciais de outro colaborador.

O titular da conta é o colaborador designado, que será responsável pelo seu uso e por todas as transações realizadas através dela.

O uso de nomes de usuários de grupos (e-mails genéricos como financeiro@empresa.com.br, compras@empresa.com.br, entre outros) não é proibido, desde que o colaborador responsável pela conta se identifique de forma clara e individualizada. Para garantir a transparência e a rastreabilidade exigidas pela LGPD, é obrigatória a identificação do usuário por meio de assinatura corporativa padronizada, conforme modelo disponibilizado pela empresa, sendo vedado o uso anônimo ou sem rastreabilidade.

Em caso de dúvidas, deve-se observar o disposto no item 6.14 da presente política.

6.10.1 Continuidade e integridade de dados corporativos

No ato da contratação, mudança de área, desligamento de Colaboradores ou finalização do vínculo, devem ser revisados e ajustados os acessos físicos e lógicos de acordo com as novas funções desempenhadas para que tenham acessos somente às informações e recursos necessários ao seu novo cargo/função e tenham seu acesso cessado por conta do desligamento ou da finalização do vínculo.

Em caso de desligamento ou finalização do vínculo, os ativos de tecnologia da informação, que possuam ou não dados armazenados, devem ser descartados ou destruídos de forma segura, evitando revelação de Informações sigilosas, perda de dados ou roubo de propriedade.

Os e-mails corporativos vinculados a usuários de grupos (como financeiro@empresa.com.br, compras@empresa.com.br, entre outros) são considerados ferramentas institucionais de uso exclusivo do Grupo Disbral, destinados à comunicação e operação de processos internos e externos, podendo a companhia excluir e/ou manter parcial ou integralmente o histórico de mensagens e arquivos, de forma a garantir a continuidade operacional, a preservação de registros corporativos e a evitação de perdas de dados relevantes, conforme os princípios de necessidade, finalidade e transparência previstos na Lei Geral de Proteção de Dados Pessoais, sendo cientificados os usuários de que devem evitar e/ou descartar informações pessoais e/ou sensíveis quando do seu uso.

6.11. Responsabilidade pelas senhas

Os usuários devem aplicar boas práticas de segurança ao selecionar e usar suas senhas.

As diretrizes e controles pertinentes ao uso segura da senha são aplicados pela IN - Gestão de Acessos e Senhas.

6.12. MESA LIMPA E TELA LIMPA

Todas as informações acessadas digitalmente ou no ambiente físico devem seguir essas diretrizes.

6.12.1.1. Política de Mesa Limpa

Se o colaborador não estiver em seu local de trabalho, todos os documentos em papel, bem como a mídia de armazenamento de dados rotulada, devem ser removidos da mesa ou de outros locais (impressoras, scanners etc.) para evitar o acesso não autorizado.

6.12.1.2. Política de Tela Limpa

Se o colaborador não estiver em seu local de trabalho, todas as informações confidenciais devem ser removidas da tela e o acesso deve ser negado a todos os sistemas para os quais a pessoa tem autorização.

No caso de ausência curta (até 30 minutos), a política de limpar a tela é implementada fazendo o logout de todos os sistemas ou bloqueando a tela com uma senha. Se a pessoa se ausentar por mais de 30 minutos, a política de limpar a tela é implementada automaticamente fazendo o logout de todos os sistemas e desligando a estação de trabalho.

6.12.1.3. Proteção de instalações e equipamentos compartilhados

Os documentos que contêm informações confidenciais devem ser removidos imediatamente das impressoras, scanners e copiadoras.

O uso não autorizado de impressoras, fotocopiadoras, scanners e outros equipamentos compartilhados para cópia [especificar máquinas e sua localização] é impedido por [especificar como - por exemplo, bloqueando a instalação, uso de números PIN, senhas de acesso etc.].

6.13. USO DA INTERNET

A Internet pode ser acessada apenas por meio da rede local da organização com infraestrutura adequada e proteção de firewall. O acesso direto à Internet através de modems externos, Internet móvel, rede sem fio ou outros dispositivos para acesso direto à Internet é proibido.

A equipe de TI pode bloquear o acesso a algumas páginas da Internet para usuários individuais, grupos de usuários ou todos os funcionários do Grupo Disbral. Se o acesso a algumas páginas da web for bloqueado, o usuário pode formalizar o pedido de liberação por e-mail a equipe de TI para autorização de acesso a tais páginas. O usuário não deve tentar contornar essa restrição de forma autônoma.

O usuário deve considerar as informações recebidas por meio de sites não verificados como não confiáveis. Essas informações podem ser usadas para fins comerciais somente após a verificação de sua autenticidade e exatidão.

O usuário é responsável por todas as consequências possíveis decorrentes do uso não autorizado ou inadequado de serviços ou conteúdo da Internet.

6.14. USO DO E-MAIL CORPORATIVO

Métodos de troca de mensagens diferentes do e-mail também incluem download de arquivos da Internet, transferência de dados via nuvens públicas, telefones, envio de mensagens SMS, mídia portátil, fóruns e redes sociais.

A direção do Grupo Disbral determina o canal de comunicação que pode ser usado para cada tipo de dado, bem como possíveis restrições sobre quem pode usar a comunicação pelos canais.

Os usuários só podem enviar mensagens contendo informações verdadeiras. É proibido o envio de materiais com conteúdo perturbador, desagradável, sexualmente explícito, rude e calunioso ou qualquer outro conteúdo inaceitável ou ilegal.

Os usuários não devem enviar mensagens de spam a pessoas com as quais nenhuma relação comercial foi estabelecida ou a pessoas que não solicitaram tais informações.

Caso o usuário receba um e-mail de spam, deverá marcá-la como spam no seu gerenciador de e-mail.

O usuário deve salvar mensagens contendo dados significativos para os negócios da organização usando o método especificado pelo analista de infraestrutura.

Cada mensagem de e-mail deve conter um aviso de isenção de responsabilidade, exceto mensagens enviadas por meio de sistemas de comunicação determinados pela direção. Se um usuário postar uma mensagem em um sistema de troca de mensagens (redes sociais, fóruns etc.), ele deve declarar inequivocamente que essa mensagem não representa o ponto de vista do Grupo Disbral.

Todos os colaboradores deverão utilizar a assinatura do Grupo Disbral para mensagens relacionadas ao negócio da empresa.

A assinatura de e-mail deverá conter a nota de confidencialidade abaixo:

Nota de Confidencialidade: Esta mensagem destina-se apenas ao destinatário indicado e pode conter informações confidenciais, proprietárias ou legalmente privilegiadas. Pessoas ou entidades não autorizadas não têm permissão para acessar essas informações. Qualquer disseminação, distribuição ou cópia dessas informações é estritamente proibida. Se você recebeu esta mensagem por engano, avise o remetente por e-mail de resposta e exclua esta mensagem e quaisquer anexos. Obrigado.

6.15. DIREITOS AUTORAIS

Os usuários não devem fazer cópias não autorizadas de software de propriedade do Grupo Disbral, exceto nos casos permitidos por lei, pelo proprietário ou diretoria.

Os usuários não devem copiar software ou outros materiais originais de outras fontes e são responsáveis por todas as consequências que possam surgir sob a lei de propriedade intelectual.

6.16. DISPOSITIVOS MÓVEIS

Dispositivo móvel inclui todos os tipos de computadores portáteis, telefones móveis, smartphones, cartões de memória e outros equipamentos móveis usados para armazenamento, processamento e transferência de dados.

6.16.1.1. Regras básicas

Um cuidado especial deve ser tomado quando o dispositivo móvel de propriedade do Grupo Disbral for colocado em carros ou outras formas de transporte, espaços públicos, quartos de hotel, locais de reunião, centros de convenção e outras áreas desprotegidas fora das instalações da empresa.

O colaborador que leva o equipamento de computação móvel para fora da empresa deve seguir estas regras:

a) Equipamentos de computação móvel que transportam informações importantes, sensíveis ou críticas não devem ser deixados sem supervisão e, se possível, devem ser fisicamente trancados, ou travas especiais devem ser usadas para proteger o equipamento
b) Ao usar equipamento de computação móvel em locais públicos, o usuário deve tomar cuidado para que os dados não possam ser lidos por pessoas não autorizadas
c) Atualizações de patches e outras configurações do sistema devem ser realizadas sempre que possível.
d) O antivírus deve estar habilitado e com as atualizações habilitadas.
e) A pessoa que usa equipamento de computação móvel externo é responsável por backups regulares de dados.
f) Não utilizar redes WiFi públicas para acessar os sistemas do Grupo Disbral.
g) No caso de equipamento de computação móvel ser deixado sem supervisão, as regras para equipamento de usuário sem supervisão devem ser aplicadas de acordo com a Política de mesa limpa e tela limpa.

A equipe de TI é responsável por treinar e conscientizar as pessoas que usam equipamentos de computação móvel fora das instalações da organização.

6.17. TRABALHO REMOTO

Trabalho remoto significa que equipamentos de informação e comunicação são usados para permitir que os funcionários realizem seu trabalho fora das instalações físicas do Grupo Disbral. O trabalho remoto não inclui o uso de telefones celulares fora das dependências da empresa.

O trabalho remoto deve ser autorizado pela Direção da empresa.

A equipe de TI é responsável por preparar planos e procedimentos para garantir o seguinte:

a) Proteção de equipamento de computação móvel conforme especificado na seção anterior
b) Prevenção do acesso não autorizado de pessoas que moram ou trabalham no local onde a atividade de teletrabalho é realizada
c) Configuração apropriada da rede local usada para se conectar à Internet
d) Proteção dos direitos de propriedade intelectual da organização, seja para software ou outros materiais que possam estar protegidos por direitos de propriedade intelectual

e) Processo de devolução de equipamentos e dados em caso de rescisão do contrato de trabalho
f) Nível mínimo de configuração da instalação onde as atividades de teletrabalho serão realizadas
g) Tipos de atividades permitidos e proibidos

6.18. CLASSIFICAÇÃO E MANUSEIO DAS INFORMAÇÕES

As informações tratadas pelo Grupo Disbral são classificadas conforme seu grau de sensibilidade, valor estratégico e impacto potencial em caso de divulgação indevida, em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e boas práticas de segurança da informação. Os níveis de classificação são:

- **Pública**: Informações expressamente autorizadas para divulgação irrestrita pelo responsável, cuja exposição externa não compromete os interesses da organização. Não requerem medidas específicas de proteção.
  Exemplos: Editais de licitação; Catálogos de serviços.
- **Interna**: Informações destinadas exclusivamente ao uso interno pelos colaboradores do Grupo Disbral, necessárias para a execução das atividades rotineiras. Não devem ser compartilhadas com o público externo.
  Exemplos: Memorandos; Políticas e procedimentos internos; E-mails e ramais; Campanhas internas.
- **Confidencial**: Informações cujo acesso é restrito a determinados colaboradores, cuja divulgação pode acarretar riscos à privacidade, violação de acordos de confidencialidade ou prejuízos à organização.
  Exemplos: Processos judiciais; Dados cadastrais de funcionários; Informações contábeis.
- **Confidencial Restrito**: Informações de alto valor estratégico, acessíveis apenas a colaboradores previamente autorizados, como diretores e gerentes. A divulgação não autorizada pode causar impactos significativos à operação ou à imagem da empresa.
  Exemplos: Atas de reuniões da diretoria; Indicadores estratégicos; Resultados de auditorias internas.

O **manuseio, armazenamento, compartilhamento e descarte** das informações devem seguir rigorosamente os critérios de classificação acima, garantindo a **confidencialidade, integridade e disponibilidade** dos dados, conforme os princípios da LGPD e da Política de Segurança da Informação do Grupo Disbral.

7. DISPOSIÇÕES FINAIS

Casos excepcionais ou não previstos serão tratados pela direção do Grupo Disbral.

8. ATUALIZAÇÃO

Esta política será reavaliada a cada 4 (quatro) anos ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.

9. APROVAÇÃO

Esta Política foi aprovada pelo Comitê de Compliance do Grupo Disbral.

Em caso de dúvidas, entre em contato com nosso Encarregado de Proteção de Dados através do e-mail dpo@disbral.com.br.