POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

1. OBJETIVOS E PRINCÍPIOS DA POLÍTICA	4
2. APLICABILIDADE	5
3. BOAS PRÁTICAS	5
3.1 Mesa Limpa.....	5
3.2 Tela limpa.....	5
3.3 Regras de segurança para o uso de BYOD (Bring Your Own Device – Traga seu próprio dispositivo)	6
3.4 Recursos de TI da Empresa	7
3.5 Regras de utilização dos recursos de TI	7
3.6 Direitos de acesso e senhas	7
3.7 Cuidados com as senhas e responsabilidade	8
3.8 Utilização de Softwares.....	8
3.9 Proteção contra vírus de computador	9
3.10 E-mail	10
3.11 Utilização da Internet.....	11
3.12 Rede WIFI	12
3.13 Acesso à Internet	12
3.14 Demais recursos de TI.....	13
3.15 Alimentos, bebidas e afins	14
3.16 Teletrabalho.....	14
3.17 Visitantes.....	15
3.18 Obrigações dos Colaboradores	15
3.19 Formação dos Colaboradores	15
3.20 Clientes e Parceiros.....	16
4. CENTRAL DE SERVIÇOS	16
4.1 Sistemas desenvolvidos e/ou adquiridos.....	16
4.2 Auditoria e Monitoramento.....	18
4.3 Arquitetura de Segurança e Integridade	19
4.4 Terceirização de Serviços.....	19
4.5 Gerenciamento de Mudanças.....	20
4.6 Acesso Remoto	20
4.7 Acesso Físico	21
4.8 Antivírus	21
4.9 Política de Backup	21

4.9.1	Aplicabilidade	22
4.9.2	Ambientes sujeitos ao backup	22
4.9.3	Rotinas de backup	22
4.9.4	Rotina de Restauração	22
4.9.5	Validação	22
5.	AUDITORIA	23
5.1	Responsáveis pela auditoria	23
6.	PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA	23
7.	REQUISITOS LEGAIS E NORMATIVOS	25
7.1	Marco Civil da Internet	25
7.2	LGPD.....	25
7.3	ISO/IEC 27001:2022	26
7.4	ISO/IEC 27701:2019 Versão corrigida 2020	26
8.	GLOSSÁRIO	27
9.	CONTROLE DE DOCUMENTO	29

1. OBJETIVOS E PRINCÍPIOS DA POLÍTICA

Com a perspectiva de proteger os direitos dos Colaboradores e do Grupo LUME, também proteger os recursos de TI, este documento define os direitos e obrigações dos Colaboradores, apresenta os riscos envolvidos no uso de recursos de TI e recomenda regras para o uso apropriado.

É de suma importância que cada colaborador esteja ciente de como deve utilizar os recursos de TI, sempre em respeito às regras definidas neste documento, a fim de garantir que a segurança dos dados será preservada.

Este documento será disponibilizado para todos na intranet. Pode ser fornecido individualmente para cada Colaborador, mediante solicitação.

O Comitê de Segurança e Privacidade da Informação permanece à disposição dos Colaboradores para fornecer-lhes qualquer explicação sobre a utilização dos recursos de TI e informá-los sobre qualquer evolução técnica. Cada Colaborador deve manter-se informado das técnicas referentes à segurança e aos avanços técnicos e tecnológicos.

Sempre que existir qualquer alteração na política de segurança da informação, o Comitê de Segurança e Privacidade da Informação comunicará a todos sobre as novas diretrizes.

O Grupo LUME está empenhado em implementar a política de segurança da informação, a fim de garantir a melhor segurança possível dos recursos de TI disponibilizados aos Colaboradores.

Qualquer uso dos recursos de TI do Grupo LUME implica que o Colaborador concorda em respeitar estritamente as regras, tal como apresentado neste documento. O uso de recursos de TI do Grupo LUME está sujeito à autorização. Quaisquer direitos de acesso concedidos são estritamente pessoais e não podem ser transferidos para outra pessoa ainda que temporariamente, sem autorização do titular, exceto em casos específicos.

Como parte do dever de todo Colaborador, é obrigatório manter sigilo das informações de sua competência e/ou conhecimento, estejam elas armazenadas em qualquer meio, seja ele físico ou digital, conforme acordado nas relações de trabalho, políticas e manuais internos, comprometendo-se neste aspecto (manter sigilo) sobre toda e qualquer informação que venham a conhecer em função de suas atividades dentro do Grupo LUME.

Todos os Colaboradores devem ter ciência que:

- a) Deverão participar de treinamentos (quando houver) a respeito dos procedimentos de segurança da informação e do uso correto das informações, instalações, desde a coleta, uso, guarda, processamento, transmissão, recepção, dentre outras operações de tratamento de dados, até o descarte.

- b) Devem informar imediatamente seu superior imediato e/ou o Comitê de Segurança e Privacidade da Informação quando informações ou aplicações críticas forem encontradas sem o tratamento de segurança correto.
- c) O Comitê de Segurança e Privacidade da Informação deve ser comunicado imediatamente quando for encontrada alguma infração às normas citadas e devem avaliar a situação e tomar as medidas cabíveis em conjunto com a gestão do Colaborador responsável pela infração.
- d) Precisam manter sigilo sobre qualquer informação que ainda não seja do conhecimento do mercado, e que todos os Colaboradores são responsáveis por manter esse sigilo.

2. APLICABILIDADE

Todos os colaboradores do GRUPO LUME.

3. BOAS PRÁTICAS

3.1 Mesa Limpa

Os Colaboradores devem manter qualquer documento com informações críticas ou com dados pessoais de terceiros em lugar seguro.

É de obrigação de cada Colaborador manter a mesa limpa e deixar sob a mesa apenas o que realmente deve usar durante o dia, assim é possível ter um controle maior sobre os papéis sobre a mesa.

Qualquer mudança de local, mesa ou posição deve ser aberto uma Requisição de Serviços, para que as devidas mudanças dos computadores sejam realizadas, mantendo-se a rastreabilidade, mantendo-se os dados e integridade dos equipamentos.

No uso das salas de reuniões, o “dono” da reunião deve se responsabilizar por verificar se ao final de uma reunião a sala está limpa e sem nenhuma informação que comprometa o Grupo LUME.

Deve-se ter muito cuidado ao imprimir uma folha com dados pessoais, a qual deve ser imediatamente recolhida por quem a imprimir, de modo que não fiquem vulneráveis ao acesso de terceiros. Antes de imprimir, deve-se verificar a sua real necessidade, sempre com o intuito de economizar com as impressões, ajudar a natureza e diminuir o risco de deixar alguma folha solta com informações importantes pelo Grupo LUME.

3.2 Tela limpa

Tela Limpa, ou "Clean Desk Policy", refere-se às práticas adotadas para assegurar que informações sensíveis e materiais confidenciais não sejam deixados expostos em áreas de trabalho quando não estiverem em uso ou após o expediente.

Este conceito se estende para as telas de computadores, onde medidas são tomadas para garantir que informações sensíveis não sejam exibidas desnecessariamente, e estejam protegidas contra visualizações não autorizadas.

Os Colaboradores nunca devem deixar o computador com a sessão aberta e desbloqueado. Ao se ausentar da estação de trabalho, bloquear a tela utilizando a combinação de teclas CTRL+ALT+DEL ou Tecla Windows+L.

Além disso, os Colaboradores devem sempre procurar encerrar as sessões que não estão sendo utilizadas e/ou efetuar a desconexão de serviços de rede ou aplicações, quando não for mais necessário.

A opção de proteção automática de tela protegida por senha, após o tempo máximo de 10 (dez) minutos sem uso, será habilitada automaticamente em todos os equipamentos ou sistemas da Grupo LUME, desde que permitam este recurso. Essa ação não invalida as responsabilidades presentes nos itens acima, sobre a necessidade de manter o computador bloqueado quando não estiver em uso ou o Colaborador se ausentar da sua mesa, as quais são prioritárias em relação ao bloqueio automático.

3.3 Regras de segurança para o uso de BYOD (Bring Your Own Device – Traga seu próprio dispositivo)

- a) Os dados corporativos só podem ser criados, processados, armazenados e comunicados de forma online na Ferramenta de Produtividade determinada pelo Grupo LUME.
- b) O Grupo LUME pode vir a requisitar que os dispositivos móveis executem programas com acessos privilegiados.
- c) Os proprietários que se recusam a permitir que a TI instale esses programas não poderão ter acesso aos dados que são protegidos por esses programas.
- d) Os dispositivos móveis devem usar formas apropriadas de autenticação de dispositivo aprovadas pela Central de Serviços, como certificados digitais criados para cada dispositivo específico. Os certificados digitais não devem ser copiados ou transferidos entre dispositivos.
- e) Os usuários BYOD devem usar formas apropriadas de autenticação de usuário aprovadas pelas políticas internas do grupo, como IDs de usuário, senhas e dispositivos de autenticação.
- f) Não é permitido dados corporativos não temporários armazenados na máquina (em qualquer dispositivo ou armazenamento não oficial).
- g) A organização tem o direito de controlar suas informações. Isso inclui o direito de backup, recuperar, modificar, determinar o acesso e/ou excluir dados corporativos sem referência ao proprietário.
- h) O Grupo LUME tem o direito de apreender e examinar forense qualquer dispositivo que se acredite conter, ou ter contido, dados corporativos quando necessário para investigação ou controle próprios.

- i) Software antivírus adequado deve ser instalado corretamente e executado em todos os dispositivos BYOD.
- j) A Central de Serviços não possui recursos ou experiência para dar suporte a todos os possíveis dispositivos e software, portanto, dispositivos usados para BYOD receberão suporte limitado em um 'melhor esforço' apenas para fins de trabalho.

3.4 Recursos de TI da Empresa

Os recursos de TI são os meios disponibilizados para cada colaborador a fim de cumprir as atividades que lhe são confiadas. Esses equipamentos devem ser utilizados apenas para uso profissional, ou seja, para evitar que o Grupo LUME esteja sujeito a problemas como ataques cibernéticos ou algo parecido. A Central de Serviço permitirá somente a instalação de softwares homologados e deve garantir a segurança desses equipamentos. Contas de e-mail particulares ou arquivos pessoais não devem estar nesses equipamentos.

3.5 Regras de utilização dos recursos de TI

Os recursos de TI disponibilizados, juntamente com todos os arquivos criados pelo Colaborador legitimamente, são de propriedade exclusiva do Grupo LUME.

Cada Colaborador deve garantir a segurança individual dos recursos de TI que lhe foram concedidos. Para isso, devem ser respeitadas as seguintes regras:

- a) Não alterar os parâmetros do sistema.
- b) Não abrir os equipamentos, pois isso pode fazer com que o Grupo LUME perca a garantia do equipamento.
- c) Não adicionar ou utilizar softwares piratas ou softwares baixados da internet sem o consentimento da Central de Serviços.
- d) Não instalar equipamentos que podem ser utilizados para estabelecer conexões de acesso livre à Internet.
- e) Certificar-se de que computadores e redes externas (como a Internet) não colocam em risco a segurança dos recursos de TI.
- f) Informar a Central de Serviços sobre qualquer anomalia operacional ou qualquer problema não resolvido.

3.6 Direitos de acesso e senhas

Direitos de acesso e senhas são fornecidos assim que o Colaborador assume sua função, de acordo com as tarefas delegadas. Os direitos de acesso podem ser limitados ou livremente removidos pelo Grupo LUME, sendo que o colaborador será informado da alteração. Os direitos de acesso de um colaborador são removidos assim que ele deixa o Grupo LUME.

Cada colaborador receberá seus acessos individualmente e assim eles devem permanecer. Os acessos e senhas são exclusivamente pessoais para o colaborador e não devem ser compartilhados. Por ser possível rastrear quem acessou e de onde acessou, isso pode gerar ao colaborador medidas administrativas punitivas,

dependendo da situação. E por ser de responsabilidade do colaborador os cuidados com esses acessos e senhas é essencial que, ao notar qualquer atividade suspeita em seus acessos, comunique imediatamente ao CISO ou ao Comitê de Segurança e Privacidade da Informação.

3.7 Cuidados com as senhas e responsabilidade

As senhas não devem ser impressas e escritas, muito menos identificadas ou registradas próximas ao computador e às estações de trabalho. Devem ser mantidas, se necessário, e de maneira não rotineira, em uma área segura de acesso exclusiva do colaborador.

Para garantir a segurança de todos, a senha deve ser “forte” e deve-se respeitar as características presentes na Política de Senhas (CS-SUP-PO-Politica_de_Senhas).

É de responsabilidade do colaborador os cuidados com a manutenção de segurança e sigilo da senha, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não devendo ser divulgadas em nenhuma hipótese.

As contas com privilégios administrativos das bases de dados serão concedidas apenas para a Central de Serviços, com assinatura do “Termo de Responsabilidade de Acesso e Concessão de Acesso ao Banco de Dados do Grupo LUME”. A reinicialização (reset) de senha (de uma base de dados) deve ser solicitada a Central de Serviços, por meio de chamado técnico e mediante análise e aprovação do gestor imediato do solicitante.

3.8 Utilização de Softwares

É proibido:

- a) Utilizar em um equipamento pessoal softwares adquiridos pelo Grupo LUME sem autorização da mesma.
- b) Fornecer a terceiros os programas de software que o Grupo LUME tenha adquirido licença.
- c) Instalar programas de jogos em um dispositivo móvel, computador ou servidor pertencente ao Grupo LUME.
- d) Utilizar os recursos de backup do Grupo LUME para arquivos privados ou pessoais (fotos, filmes etc.).
- e) Utilizar programas de software que o Grupo LUME não tenha adquirido a licença ou utilizar cópias ilegais.
- f) Baixar e/ou instalar qualquer software da internet ou qualquer outro serviço on-line nos computadores ou servidores.
- g) Utilizar softwares para os quais o colaborador possui uma licença pessoal nos equipamentos pertencentes ao Grupo LUME.

- h) Utilizar softwares de “shareware” após o vencimento do período experimental, salvo se o Grupo LUME prolongar esse período.
- i) Instalar ou utilizar qualquer software de criptografia em computadores pertencentes ao Grupo LUME, salvo se houver autorização prévia por escrito da Central de Serviços.
- j) Adquirir software sem avaliação prévia e autorização expressa da Central de Serviços.
- k) Instalar aplicativo nas estações de trabalho sem a homologação do Grupo LUME por meio da Central de Serviços, seja ele comercial, freeware ou shareware.
- l) Utilizar software não adquirido oficialmente pelo Grupo LUME bem como cópias não licenciadas, autorizadas e homologadas pela Central de Serviços.
- m) Utilizar equipamentos pessoais sem a autorização do gestor.

Todos os programas existentes nas estações de trabalho devem ser homologados pela Central de Serviços sob o ponto de vista técnico/operacional, controlados para efeito de inventário e disponibilidade. Exceções devem ser comunicadas a Central de Serviços para tomada das providências necessárias a fim de garantir a utilização do recurso dentro do nível de segurança definido pelo Grupo LUME.

Todas as instalações devem ser monitoradas e a Central de Serviços poderá fazer uma auditoria nos equipamentos para verificar eventual software ou aplicação instalados de forma ilegal. Se assim constar, haverá remoção automática e o colaborador será advertido.

3.9 Proteção contra vírus de computador

Para prevenir a invasão e propagação de vírus, não devem ser utilizadas unidades removíveis (pendrives, gavetas USB ou qualquer outro tipo de mídia removível) sem antes haver uma varredura por antivírus.

Quaisquer documentos ou programas que um colaborador receber por meio magnético ou óptico, ou baixado da internet, deve obrigatoriamente ser analisado para detectar possíveis vírus e outros programas destrutivos. Essa análise deve ser realizada utilizando softwares de antivírus fornecidos pelo Grupo LUME.

Somente softwares de antivírus aprovados devem ser utilizados para prevenir contra vírus. Além disso, os colaboradores devem alertar a Central de Serviços caso apareça alguma mensagem do antivírus em seu computador ou dispositivo.

É proibido instalar e/ou desabilitar seu antivírus, a menos que você receba autorização prévia e expressa da Central de Serviços.

3.10 E-mail

O e-mail deve ser utilizado exclusivamente para troca de mensagens que atendam às funções operacionais do Grupo LUME.

Todo conteúdo confidencial e sigiloso veiculado por e-mail poderá utilizar técnicas de criptografia ou qualquer outra disponibilizada pelo Grupo LUME para este fim visando proteger sua confidencialidade e integridade.

Se houver desconfiança de algum e-mail, o colaborador não deve abri-lo e deve acionar a Central de Serviço para validação, pois existem e-mails conhecidos como phishing que são e-mails falsos utilizados apenas para capturar e/ou roubar as informações do computador.

Utilize o e-mail somente enquanto estiver trabalhando. O colaborador deve estar ciente de que, embora execute função ou trabalho externo, sem horário fixo, deve garantir seu horário de descanso e lazer, não trabalhando ou enviando e-mails em horários noturnos, finais de semana ou feriados, exceto quando solicitado por seu gestor.

É de responsabilidade do colaborador cuidar da integridade, confidencialidade e disponibilidade das informações contidas em seu e-mail, devendo comunicar por escrito ao superior imediato quaisquer indícios ou possibilidades de irregularidades.

As informações contidas em sua caixa de e-mail são do Grupo LUME, o que não lhe dá o direito de compartilhar as informações contidas nele com outras pessoas de fora do Grupo LUME, a não ser para tratativas profissionais (relacionadas ao trabalho em execução).

O colaborador deve alterar sua senha sempre que obrigatório ou que tenha suspeita de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas. Deve, ainda, respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados no Grupo LUME.

A configuração dos e-mails segue alguns parâmetros de segurança:

- a) Acesso às caixas de e-mail do Grupo LUME é autenticado e relacionado a um colaborador.
- b) Os e-mails trocados entre o Grupo LUME e terceiros usam criptografia para segurança da informação e dos envolvidos.
- c) Envio ou recebimento de e-mails para caixas de e-mails ou sistemas de mensagens do Grupo LUME só podem ser realizados para fins profissionais, podendo ser auditados e preservados pelo período de um ano.
- d) As caixas de e-mails estão sujeitas ao registro de eventos.

Qualquer e-mail que passa por meio da caixa de e-mails disponibilizados para colaboradores é considerado de natureza profissional.

Excepcionalmente, o colaborador tem o direito de usar e-mails disponibilizados pelo Grupo LUME para fins privados, desde que autorizado pelo gestor.

Cada colaborador deve ter cuidado para não usar mensagens eletrônicas de forma abusiva e desproporcional. É expressamente proibido:

- a) Envio de mensagens sem identificar a origem ou utilizando-se de conta de e-mail de outras pessoas.
- b) Envio de mensagens com conteúdo difamatório, ofensivo, discriminatório, homofóbico ou afins, que importune ou cause constrangimento às pessoas.
- c) Envio de mensagens com vírus arquivos do tipo “Cavalo de Tróia” e mensagens não solicitadas, como “spam”, “junk mails” e correntes.

Atenção: e-mails internos do Grupo LUME são seguros. No entanto, e-mails que passam pela internet podem, a qualquer momento, ser interceptados, exibidos, salvos e utilizados para fins não autorizados por terceiros.

3.11 Utilização da Internet

A Internet é um recurso de TI fornecido pelo Grupo LUME com o objetivo de aumentar a produtividade dos processos de trabalho, devendo seu uso ser exclusivo para atividades do Grupo LUME. É proibido a consulta e/ou veiculação de imagens ou informações que não estejam relacionadas para o fim profissional.

A liberação de acesso é feita pela Central de Serviço e é auditada para fins de controle. Os acessos serão fornecidos de acordo com cada departamento e em caso de solicitação de liberação de novos acessos é necessário abrir uma Requisição de Serviço para que a Central de Serviços analisar a solicitação.

O acesso à Internet para algumas operações rotineiras, como acesso a sites de bancos, será permitido. Todo acesso é auditado e o abuso desses acessos será reportado para o gestor do colaborador.

É vedado o uso ou reprodução de qualquer material da Internet, incluindo softwares, gráficos, áudio, vídeo e similares que o Grupo LUME não tenha propriedade intelectual e/ou licença, sem que haja prévia e formal aprovação dos proprietários dos direitos.

É vedada a utilização do acesso à Internet para participação em campanhas cívico-sociais, adesão a programas de ajuda mútua (pirâmides, correntes etc.), aquisição de qualquer tipo de bem ou serviço de uso particular e outras atividades similares.

O colaborador violará as regras do Grupo LUME se utilizar os recursos de TI para visualizar, enviar informações sobre, ou consultar sites cujo conteúdo vai contra a ordem pública ou aos bons costumes, particularmente os sites com conteúdo que é xenófobo, homofóbico, racista, revisionista ou pedófilo.

3.12 Rede WIFI

A rede WIFI do Grupo LUME é dividida da seguinte forma:

- a) Rede Visitantes (Grupo LUME - Visitantes): isolada da rede corporativa permitindo apenas acesso à internet e a e-mails de forma controlada e limitada.
- b) Rede Corporativa (Grupo LUME - Corporativo): rede com acesso aos arquivos e recursos da rede para que os Colaboradores possam executar suas atividades do dia a dia (jamais deve ser atribuída para um visitante).

O acesso para visitantes é realizado por meio de senha e a liberação se dá apenas por autorização de algum gestor.

3.13 Acesso à Internet

O acesso à Internet é controlado por categorias e definido por perfis individualmente acordados com o gestor imediato. De forma padrão, os acessos classificados nas categorias abaixo são proibidos:

- 1) Violence/Hate/Racism: Violência/Odio/Racismo
- 2) Intimate Apparel/Swimsuit: Roupa íntima/Traje de Banho
- 3) Nudism: Nudismo
- 4) Pornography: Pornografia
- 5) Weapons: Armas
- 6) Adult/Mature Content: Conteúdo Adulto/Maduro
- 7) Cult/Occult: Cultos/Ocultismo
- 8) Drugs/Illegal Drugs: Drogas/Drogas Ilegais
- 9) Illegal Skills/Questionable Skills: Habilidades Ilegais/Habilidades Questionáveis
- 10) Sex Education: Educação Sexual
- 11) Gambling: Jogos de Azar
- 12) Alcohol/Tobacco: Álcool/Tabaco
- 13) Chat/Instant Messaging (IM): Chat/Mensagens Instantâneas
- 14) Arts/Entertainment: Artes/Entretenimento
- 15) Business and Economy: Negócios e Economia
- 16) Abortion/Advocacy Groups: Aborto/Grupo de Defesa
- 17) Education: Educação
- 18) Cultural Institutions: Instituições Culturais
- 19) Online banking: Banco online
- 20) Games: Jogos
- 21) Government: Governo
- 22) Military: Militar
- 23) Political/Advocacy Groups: Grupo Políticos/Advocacia

- 24) Health: Saúde
- 25) Information Technology/Computers: Tecnologia da Informação/Computadores
- 26) Hacking/Proxy Avoidance Systems: Hacking/Sistemas de Evitação de Proxy
- 27) Search Engines and Portals: Motores de Busca e Portais
- 28) E-mail: E-mail
- 29) Web Communications: Comunicações Web
- 30) Job Search: Busca de Emprego
- 31) News and Media: Notícias e Mídia
- 32) Personals and Dating: Pessoais e Namoro
- 33) Usenet News Group: Grupo de Notícias Usenet
- 34) Reference: Referência
- 35) Religion: Religião
- 36) Shopping: Compras
- 37) Internet Auctions: Leilões na Internet
- 38) Real Estate: Imóveis
- 39) Society and Lifestyle: Sociedade e Estilo de Vida
- 40) Restaurants and Dining: Restaurantes e Jantar
- 41) Sports/Recreation: Esportes/Recreação
- 42) Travel: Viagem
- 43) Vehicles: Veículos
- 44) Humor/Jokes: Humor/Piadas
- 45) Multimedia: Multimídia
- 46) Freeware/Software Downloads: Freeware/Downloads de Software
- 47) Pay to Surf Sites: Sites de Pagamento para Navegar
- 48) Kid Friendly: Amigável para Crianças
- 49) Advertisement: Publicidade
- 50) Web Hosting: Hospedagem na Web
- 51) Other: Outros
- 52) Internet Watch Foundation CAIC: Fundação de Observação da Internet CAIC
- 53) Social Networking: Redes Sociais
- 54) Malware: Malware
- 55) Radicalization and Extremism: Radicalização e Extremismo

Para liberação de acesso via Internet a locais classificados nas categorias acima, deve ser solicitada formalmente a Central de Serviços, via sistema de chamados técnicos, mediante análise e aprovação da Central de Serviço e do gestor imediato do colaborador solicitante.

3.14 Demais recursos de TI

É de responsabilidade de todos os colaboradores:

- a) O uso correto dos recursos de TI disponibilizados pelo Grupo LUME.
- b) O uso correto dos recursos de TI disponibilizados de forma dedicada, cabendo ao colaborador beneficiado zelar pelos aspectos de manutenção, proteção

física, controle de acesso lógico e uso adequado para as finalidades a que foi designado.

- c) No caso de furto ou roubo de um recurso de TI disponibilizado de forma dedicada ao colaborador pelo Grupo LUME, notificar imediatamente o gestor e a Central de Serviço, além de acionar as autoridades policiais por meio de boletim de ocorrência (B.O.), no prazo máximo de 4 (quatro) dias corridos contados do incidente.

Em casos de danos/avarias decorrentes do mau uso do equipamento sob responsabilidade do colaborador, a Central de Serviço o enviará ao fornecedor homologado para fins de orçamento e manutenção, sendo o valor descontado conforme descrito no Termo de Responsabilidade assinado em sua entrega (ADM-BACK-FO-Termo_Entrega_Ativos).

A Central de Serviços é responsável pelo inventário dos equipamentos, aplicativos e softwares do Grupo LUME, assim como por auditorias regulares para avaliar a utilização (CS-SUP-RE-Gestao_de_Ativos).

Toda contratação de sistemas, serviços e/ou tecnologia deverá ser analisada pela Central de Serviços, o qual deverá fazer uma avaliação levando em consideração requisitos de segurança, desempenho, benefícios etc., bem como a sua capacidade técnica (CS-SUP-FO-Check_List_SI_Aquisicao).

A Central de Serviços poderá inspecionar toda e qualquer informação (como por exemplo: e-mails, arquivos, diretórios etc.) que transite ou esteja armazenada na sua rede ou ainda em qualquer dispositivo pertencente ao Grupo LUME ou por esta autorizado a ser utilizado para fins profissionais por qualquer colaborador.

Acesso e uso da rede, e-mails e sistemas serão bloqueados durante o período de afastamento do colaborador (descanso remunerado, licença, entre outras) e seus e-mail serão direcionados a pessoa indicada ao PX-People Experience que irá solicitar a aplicação através de Requisição de Serviços técnico enviado a Central de Serviços. Exceção: Cargos de confiança não terão seu acesso bloqueado.

3.15 Alimentos, bebidas e afins

É expressamente proibido o consumo de alimentos, bebidas ou algo do gênero em locais de área segura, assim como fumar ou realizar atividades que não sejam relacionadas à manutenção, controle e utilização do ativo. Além disto, recomenda-se expressamente que alimentos, bebidas e afins não fiquem em contato ou em proximidade perigosa com ativos de informação ou TI.

3.16 Teletrabalho

Os equipamentos portáteis e/ou aqueles utilizados em teletrabalho ou externamente deverão ter um cuidado adicional, de forma que preservem a informação neles contida.

Apenas pessoal autorizado pode realizar seu trabalho fora da organização. O teletrabalho pode incluir o uso de telefones celulares fora das instalações da organização, desde que seja uma linha da empresa.

A Central de Serviço é responsável pela preparação dos planos e procedimentos se for considerado necessário para garantir o seguinte:

- a) Proteção dos equipamentos de informática móvel.
- b) Impedir o acesso não autorizado de pessoas que vivam ou trabalhem no local onde ocorre a atividade de teletrabalho.
- c) Configuração adequada da rede local usada para se conectar à Internet.
- d) Proteção dos direitos de propriedade intelectual da organização, tanto para o software quanto para outros conteúdos que podem ser protegidos por direitos de propriedade intelectual.
- e) Processo de devolução de dados e equipamentos em caso de rescisão do contrato de trabalho (em conjunto com o PX - People Experience).
- f) Nível mínimo de configuração da instalação onde serão realizadas as atividades de teletrabalho.

3.17 Visitantes

Os visitantes, devem ser acompanhados pelo responsável em todo tempo que estiverem dentro das instalações do Grupo Lume, além disto, a entrada e a saída devem ser registradas para controle.

3.18 Obrigações dos Colaboradores

O colaborador deve informar imediatamente ao Comitê de Segurança e Privacidade da Informação qualquer tentativa de violação da sua estação de trabalho ou arquivos, informações ou dados, para que se possa investigar quem é responsável por quaisquer incidentes que possam ocorrer.

Em casos de roubo de computador, celular ou arquivos de backup, ou violação de quaisquer recursos de TI disponibilizados ao colaborador, o Comitê de Segurança e Privacidade da Informação deve ser imediatamente informado.

O colaborador deve responder, em todas as instâncias, pelas consequências das ações ou omissões de sua responsabilidade que possam pôr em risco ou comprometer a exclusividade de sua senha ou das transações a que tenha acesso.

3.19 Formação dos Colaboradores

O Grupo LUME, através do Comitê de Segurança e Privacidade da Informação, proporcionará aos colaboradores treinamentos e/ou atividades de conscientização sobre ameaças de segurança cibernética e melhores práticas individuais, os quais podem ser realizados por qualquer meio apropriado (mensagens, intranet, telas,

exercícios etc.), em conformidade com as políticas ou padrões de comunicação internos do Grupo LUME.

Além disso, os colaboradores devem, regularmente (pelo menos uma vez por ano), consultar e validar os termos de uso dos sistemas de informação sujeitos a esse documento.

3.20 Clientes e Parceiros

Caso disponível, encaminhada e treinada, os colaboradores do Grupo LUME, além de seguirem esta política, devem seguir as políticas de segurança do Cliente em questão. Sempre ao atender, os colaboradores do Grupo LUME devem observar principalmente as questões de segurança da informação pertinentes como encaminhamento de senhas e permissão autorizadas para os usuários em questão, o compartilhamento ou envio de informações somente deverá se dar para usuários autorizados para tal fim.

4. CENTRAL DE SERVIÇOS

Como responsável pelos recursos de TI utilizados pelo Grupo LUME, a Central de Serviços deve tomar alguns cuidados a mais quando o assunto é segurança. Por esse motivo este tópico é dedicado especialmente à equipe de TI para tomada das melhores decisões baseadas em conhecimento.

4.1 Sistemas desenvolvidos e/ou adquiridos

Todo e qualquer sistema criado ou adquirido deve ser baseado em perfil de acesso, ou seja, deve atribuir acessos específicos para cada perfil, garantindo assim a segurança dos sistemas. Sistemas legados que não possuem perfil de acesso devem ser trocados ou deve ser implementada a função de perfil de acesso.

Antes de instalar uma ferramenta é importante mapear todos os acessos e documentá-los, sendo que esses registros devem ser avaliados e autorizados pelos gestores de cada área responsável.

A implementação de sistemas e ferramentas deve ser sempre a mais restrita possível, garantindo maior segurança e concedendo liberações somente quando realmente necessário. Essas liberações devem ser atribuídas ao perfil de acesso, e não ao colaborador, para manter a rastreabilidade dos acessos.

A customização de senhas é obrigatória e deve seguir pelo menos as seguintes características:

- a) Definição de tempo para bloqueio ou expiração de contas e/ou senhas.
- b) Definição do número máximo de tentativas de acesso incorretas consecutivas com bloqueio de contas e/ou senhas.
- c) Senha com no mínimo de 8 (oito) caracteres.

- d) Senha com pelo menos 4 (quatro) tipos de caracteres (letras minúsculas, letras maiúsculas, números e símbolos).

O número máximo de tentativas de autenticação sem sucesso nos sistemas (logon) é de 3 (três) vezes, sendo que, ultrapassado esse número, a conta do usuário permanecerá bloqueada e a liberação será efetuada apenas por solicitação formal do seu gestor.

As senhas de acesso terão uma validade de 42 (quarenta e dois) dias, quando deve ser requisitada automaticamente a sua troca para o usuário. O usuário não poderá reutilizar as suas últimas 10 (dez) senhas.

A autorização para utilização de cada função, tela ou módulo do sistema e/ou aplicativo deverá ser realizada por usuário, e deverá ser solicitada a Central de Serviços por meio de Requisição de Serviços, mediante aprovação do gestor do colaborador envolvido.

Em rotinas que necessitam de ações de um único usuário (ex. aprovações financeiras), o sistema deve permitir delegação de função de maneira a não comprometer as atividades em caso de sua ausência, solicitada a Central de Serviços por meio de uma Requisição de Serviços e com aprovação pelo gestor da área envolvida.

Os sistemas e aplicativos devem permitir o bloqueio de acesso de forma automática, ou manual, quando da ausência temporária do usuário por motivo de férias, descanso remunerado, licença ou por motivos de força maior.

Todo acesso a sistemas/aplicativos deverá ser realizado por meio de identificação de usuário individualmente e de autenticação por senha.

Os desenvolvedores e testadores devem ter acesso apenas às fontes necessárias à execução do seu trabalho. Além disso, devem ser autenticados lógica e fisicamente ao acessar os ambientes de desenvolvimento e homologação. Não é permitido, mesmo nesses ambientes, acesso não identificado ou com conta genérica.

As contas com privilégios administrativos serão concedidas apenas para a Central de Serviços, com ciência do PX – People Experience, registradas em Requisição de Serviços pelo sistema de gestão de chamados.

Quando da criação de um usuário, a Central de Serviços criará uma senha expirada (com obrigatoriedade de troca no primeiro acesso), a qual será enviada diretamente ao usuário por meio de chamado, preferencialmente.

Os sistemas desenvolvidos ou adquiridos não devem utilizar contas administrativas ou privilegiadas (ex. root, administradores, sys etc.) de sistemas operacionais, servidores web ou banco de dados.

Os sistemas e as redes devem estar programados para desconectar o usuário por tempo de inatividade superior a 15 (quinze) minutos.

Os sistemas ou os aplicativos que necessitam estar conectados diretamente à internet (ex. portais web) deverão estar segregados física e/ou logicamente da rede corporativa (ex. por meio de firewall ou uma DMZ), com proteção por mecanismo de detecção e prevenção de intrusos, em rede própria ou terceirizada.

A extração da base de dados (ex. toda a base de consumidores, toda a base de participantes, toda a base de colaboradores, todas as transações realizadas etc.) deve ser efetuada pela Central de Serviço e com autorização formal do Comitê de Segurança e Privacidade da Informação, com o objetivo de evitar incidentes de vazamento de dados.

Após entrar em produção, sempre que possível a senha do banco deve ser dividida entre a Central de Serviço e o fornecedor que prestará o suporte.

4.2 Auditoria e Monitoramento

Todos os sistemas desenvolvidos ou adquiridos pelo Grupo LUME devem conter registros de auditoria (logs). Estes registros devem ser gravados com data/hora de ocorrência, endereço IP, hostname (endereço da estação de trabalho), conta utilizada e registro, minimamente, dos seguintes eventos:

- a) Falhas de acesso nos sistemas.
- b) Criação e a remoção de usuários.
- c) Atribuição e remoção de direitos e acessos do usuário.

Todos os sistemas deverão ter interface amigável para consulta dos logs ou possuir capacidade de encaminhar estes logs para um servidor de logs do Grupo LUME.

Todos os logs devem ser protegidos, cabendo o acesso e a possível deleção dos dados apenas a usuários com perfis específicos e restritos.

Os registros devem ser desenvolvidos e configurados de forma a evitar a exaustão da trilha de auditoria (ex. por meio de log rotation).

Além dos sistemas, todos os servidores, switches, firewall, access points devem fornecer log a fim de montar um rastreamento dos dados do ambiente.

Os logs devem ser mantidos por períodos mínimos determinados pelos gestores, devendo considerar os aspectos legais e regulatórios envolvidos, bem como as necessidades de negócio. Recomenda-se, nos casos omissos, o armazenamento dos logs por um período não inferior a 2 anos.

4.3 Arquitetura de Segurança e Integridade

Os ambientes de desenvolvimento, homologação e produção devem ser física e logicamente isolados, a fim de:

- a) Reduzir o acesso físico de pessoas externas aos ambientes.
- b) Reduzir o acesso dos desenvolvedores ao ambiente de produção.
- c) Garantir a qualidade das funções de segurança do sistema gerado.

O Datacenter ficará fechado e será permitida apenas a entrada dos colaboradores integrantes da Central de Serviços. Os racks também devem ficar fechados para garantir que, havendo visita de colaboradores ou terceiros ao Datacenter, não haverá acesso físico aos servidores. A visita ao Datacenter só será possível acompanhada por colaborador autorizado da Central de Serviços.

Caso necessário armazenamento de senhas de sistemas ou aplicativos em arquivos de sistema operacional, estes arquivos não deverão ser logicamente alocados em diretórios de servidores web, ou FTP, e seu acesso deve ser restrito para acesso apenas pela aplicação.

Não deverá existir portas lógicas ou meios alternativos (ex. backdoors, maintenance hooks) de acesso aos sistemas desenvolvidos ou adquiridos.

Todo sistema desenvolvido e adquirido pelo Grupo LUME deve preferencialmente conter mecanismos de backup e restauração dos dados processados, além de possuir capacidade de tolerância a falhas e retorno à operação. Em casos omissos, fica a Central de Serviços responsável pela elaboração de política de backup e restore dos bancos de dados e/ou arquivos dos sistemas instalados.

A Central de Serviços é responsável pelo encaminhamento de erro ao fornecedor do sistema, pelo recebimento da correção e de sua aplicação em ambiente de validação para serem realizados testes pelo usuário reclamante e, se aprovado, por meio de chamado, deverá ser solicitada a instalação da correção no ambiente de produção.

4.4 Terceirização de Serviços

O desenvolvimento terceirizado de sistema deve ser realizado em conformidade com os controles definidos nesta política de segurança da informação, e deve ser monitorado constantemente por meio da implementação de procedimentos específicos, tais como:

- a) Inclusão de termos de uso sobre licenças, propriedade de código-fonte, direitos de propriedade intelectual e confidencialidade de informações nos contratos e acordos de nível de entrega dos serviços de terceiros.
- b) Inclusão de política de privacidade e proteção de dados, especialmente dados pessoais.

- c) Certificação da qualidade, através de certificações ou cursos referentes ao trabalho a ser executado.
- d) Definição de sanções ou ações específicas para a eventualidade de falha por parte dos prestadores de serviço.
- e) Garantia de direitos de acesso para auditoria da qualidade e exatidão do trabalho executado.
- f) Definição de requisitos contratuais de qualidade e de segurança do código.

4.5 Gerenciamento de Mudanças

As mudanças ou atualizações no ambiente de produção (ex. atualização de sistema operacional, aplicação de patches etc.), quando solicitadas pelos colaboradores, devem ser revisadas previamente e testadas em ambiente de homologação, especialmente quanto aos impactos nos sistemas e aplicativos, evitando sua indisponibilidade ou falhas que possam comprometer a segurança das informações.

A aprovação das mudanças em ambiente de produção deverá ser realizada apenas após homologação e, ainda com base no resultado destes procedimentos, devendo ser formal e documentada.

A modificação em pacotes de software (adquiridos de fornecedores) deverá ser realizada apenas quando imprescindível, sendo realizadas de acordo com as seguintes condições:

- a) Deverão ser avaliados e documentados pela Central de Serviços os riscos de comprometimento dos controles embutidos e da integridade dos processos, sendo requerida, quando existentes, a sua aceitação pela gestão responsável.
- b) Deverá ser obtida autorização do fornecedor antes de implementar qualquer modificação no pacote.
- c) Deverá ser averiguada, prioritariamente, a possibilidade de obter a modificação necessária diretamente do fornecedor, como atualização padrão do programa.
- d) Deverá ser avaliado o impacto de se tornar responsável pela manutenção do software como resultado da modificação.
- e) Deverá ser mantida uma cópia da versão original do software, como garantia de rollback (retorno à instalação anterior, antes da aplicação da nova versão).
- f) Deverão ser testadas e documentadas todas as modificações, de forma que possam ser replicadas, se necessário, em futuras atualizações de software.

4.6 Acesso Remoto

A concessão de acesso externo a recursos de TI do Grupo LUME deve ser evitada e limitada à necessidade premente para execução das atividades profissionais.

O acesso remoto será concedido única e exclusivamente para as finalidades e funções que o exijam, observando-se os procedimentos formais de solicitação,

alteração, monitoramento e exclusão de acessos, bem como as restrições definidas neste e nos demais requerimentos de segurança do Grupo LUME.

As conexões de acesso remoto deverão seguir as mesmas considerações das conexões efetuadas internamente.

O acesso poderá ser liberado desde que formalmente justificado por interesses do Grupo LUME, conforme abaixo:

- a) Para colaboradores que acessam os sistemas e recursos de TI remotamente para desempenho de suas funções, deve-se solicitar formalmente a Central de Serviços, via chamado técnico, o qual aprovará ou não a solicitação mediante análise e aprovação conjunta com gestor imediato do colaborador solicitante.
- b) Para empresas parceiras e/ou fornecedores que necessitam compartilhar informações de negócios ou conectar remotamente no ambiente do Grupo LUME, deve-se solicitar formalmente a Central de Serviço, via chamado e/ou e-mail (neste caso deverá ser aberto chamado pela própria Central de Serviço para registro), a qual aprovará ou não a solicitação mediante análise e aprovação conjunta com gestor imediato do colaborador solicitante.

Os acessos autorizados devem ser feitos obrigatoriamente por meio de uma conexão segura utilizando uma ferramenta de Gerenciamento de Acesso Privilegiado (PAM).

4.7 Acesso Físico

Acesso físico aos ambientes e instalações do Grupo LUME, nos quais são obrigatórios controles de acesso, somente será possível por meio do uso de mecanismo de controle de acesso como tags, senhas, crachás e/ou biometria.

4.8 Antivírus

É de responsabilidade da Central de Serviços para os equipamentos do grupo:

- a) Manter o antivírus atualizado em todas as estações e servidores.
- b) Analisar os relatórios de vírus na rede e tomar ações corretivas e/ou treinamentos.
- c) Sempre que possível, não deixar o colaborador tomar ações no antivírus.
- d) Acionar ferramentas para atuar automaticamente na eliminação de riscos de infecção e danos.

4.9 Política de Backup

O serviço de backup é essencial para eventual restauração de arquivos e, em alguns casos, até para a restauração de todo o ambiente. Cabe a Central de Serviços manter o backup periódico e constante, bem como realizar testes de restauração para evitar surpresas quando necessário.

4.9.1 Aplicabilidade

Todas as Máquinas Virtuais do Grupo LUME.

4.9.2 Ambientes sujeitos ao backup

Para backup, deve-se considerar no mínimo os seguintes ambientes e suas criticidades:

Ambiente	Criticidade
Servidores de arquivos *	Alto
Office 365	Alto
Servidores de Banco de Dados	Alto
Demais Máquinas Virtuais ou físicas	Alto e Médio vide anexo

4.9.3 Rotinas de backup

As rotinas de backup devem seguir no mínimo as seguintes recomendações:

- Backup Incremental (diário): diariamente de segunda a segunda com retenção de 07 dias.
- Backup Database Dump Full (diário): diariamente às 20:00 horas.
- Replicação do Database Dump para o Blob Storage da Azure com retenção de 05 dias.
- Replicação LRS deve ser aplicada. O armazenamento com redundância local (LRS), copia seus dados de forma síncrona três vezes em um único local físico na região primária.

4.9.4 Rotina de Restauração

Deve-se restaurar mensalmente arquivos para testes e documentação e a restauração do ambiente em paralelo para validação do backup.

4.9.5 Validação

Deve-se validar a restauração a fim de garantir a integridade dos dados em backup.

5. AUDITORIA

A fim de garantir que as regras e normas estabelecidas neste documento serão respeitadas, serão efetuadas auditorias sobre o uso de recursos de TI, inclusive, mas não somente:

- a) Auditoria pós-incidente em casos de mau funcionamento de sistemas.
- b) Auditoria de conformidade para verificar se os recursos de TI estão sendo utilizados de forma adequada pelos colaboradores em relação à autorização que lhes foi concedida para os seus respectivos cargos.
- c) Auditoria de Sistema de Gestão para verificar se os requisitos e controles necessários para as normativas internas estão sendo cumpridos.

As auditorias serão realizadas para garantir o bom funcionamento dos sistemas, bem como proteger os dados pessoais dos colaboradores, fornecedores, terceiros e outros.

5.1 Responsáveis pela auditoria

Somente a presidência do Grupo LUME, os Heads das áreas e o Comitê de Segurança e Privacidade estão autorizados a solicitar uma auditoria interna, além das programadas pelo Programa de Auditoria Interna. As auditorias serão implementadas sob a responsabilidade da área de PX – People Experience e, quando necessário, do departamento jurídico do Grupo LUME. As auditorias de certificação, seguindo os preceitos, são de responsabilidade da certificadora escolhida, podem, ainda, ocorrer auditorias externas sob responsabilidade de consultorias, entretanto, elas só devem ocorrer mediante solicitação da presidência do Grupo LUME.

6. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

Em caso de identificação de incidente de segurança, o CISO, por meio do Comitê de Segurança e Privacidade, incluindo o DPO, deve ser imediatamente acionado para colocar em prática o Plano de Resposta abaixo:

- 1) Acionar os departamentos jurídico, de relações públicas e de PX – People Experience para atuação conjunta sobre o incidente de segurança.
- 2) Antes de tomar qualquer ação, analisar e buscar entender de qual base vazaram os dados (para isso é necessário manter em dia o mapeamento de dados e informações dos ambientes de responsabilidade do Grupo LUME).
- 3) Criar um plano de ação para descobrir a origem do vazamento.
- 4) Caso o vazamento tenha sido em massa, paralisar os sistemas.
- 5) Colocar os dispositivos afetados off-line (sem conectividade), mas não os desligar e nem realizar alterações (o objetivo é interromper qualquer atividade em andamento e limitar a comunicação dos sistemas afetados, mas sem cometer nenhuma ação que possa apagar pistas ou contaminar evidências).

- 6) Fazer dump de memória de todos os equipamentos envolvidos, além de capturar todos os logs.
- 7) Alterar as senhas (a alteração de senhas ou credenciais de bloqueio é uma tática comum na preparação para investigar uma violação de dados, pois ajuda a garantir a cessação do referido vazamento).
- 8) Aplicar os passos acima em todas as contas envolvidas, confirmadas ou suspeitas.
- 9) Colocar o ambiente off-line e determinar o impacto.
- 10) Iniciar a investigação para descobrir quais dados foram acessados, quais sistemas foram comprometidos e quais contas podem ter sido utilizadas.
- 11) Registrar as alterações de senhas, bem como as informações obtidas após a paralisação dos sistemas.
- 12) Reunir todas as informações e evidências possíveis (para determinar se houve um incidente de segurança ou vazamento de dados, é fundamental entender exatamente como quando e onde se deu o potencial incidente, pois há casos de invasão cibernética e falhas de segurança oriundas dos próprios Colaboradores).
- 13) Detectar e avaliar os dados objeto do incidente (é imprescindível entender que tipos de dados foram comprometidos, pois assim será possível avaliar precisamente o incidente e suas consequências).
- 14) Após detecção e avaliação dos dados, avaliar a real dimensão do problema e da sua gravidade.
- 15) Determinar as medidas a serem tomadas pelo Grupo LUME em decorrência do incidente, inclusive medidas de proteção e mitigação de riscos para evitar reincidência.
- 16) Planejar o próximo passo, como: mudanças de senhas, atualização de softwares, alteração de regras de firewall da rede, separação de sub-redes, execução de verificações antimalware, reforço dos registros e alertas e algumas outras etapas técnicas.
- 17) Implementar o planejamento acima.
- 18) Comunicar os detalhes do incidente aos colaboradores (não são apenas com as etapas técnicas que o Grupo LUME deve se preocupar; há também o processo de comunicação e notificação, em que todos ficam cientes do que ocorreu, como aconteceu a violação, quais dados foram vazados e o que deve e será feito).
- 19) Comunicar o incidente às pessoas externas envolvidas, mediante notificação sobre o vazamento de dados, especialmente os titulares, quando se tratar de dados pessoais).
- 20) Tomar as medidas possíveis de proteção da reputação do Grupo LUME, a qual deve ser preservada.
- 21) Agir com transparência, sempre que possível, manter as informações atualizadas e estar de prontidão para quaisquer dúvidas de titulares, vítimas e envolvidos.

- 22) Em se tratando de dados pessoais, e caso confirmado o incidente, comunicar à Autoridade Nacional de Proteção de Dados (ANPD).
- 23) Divulgar informações sobre o ocorrido e preparar a equipe envolvida para fornecer respostas (é importante, por exemplo, a depender da extensão do incidente, um porta-voz indicado fazer anúncio público na forma de uma coletiva de imprensa, e-mails ou anúncios de mídia social).
- 24) Adotar outras medidas para redução dos danos à imagem e à reputação do Grupo LUME, além de demonstrar que o problema está sendo assumido e que há comprometimento com a sua resolução.
- 25) Descrever o que o Grupo LUME fez para remediar a violação, o que ela pretende fazer no futuro e quais etapas (se houver) devem ser tomadas pelos titulares dos dados para se proteger, como alterar senhas, entrar em contato com empresas de cartão de crédito ou emitir alertas, dentre outras medidas pertinentes.
- 26) Criar uma linha direta para tratar das preocupações dos titulares dos dados em relação à violação ou incidente, para que se possa responder às perguntas e fornecer orientações de forma organizada e centralizada.
- 27) Fortalecer a prevenção, planejar e executar medidas para que o incidente não venha a acontecer novamente.
- 28) Identificar as lacunas e os pontos de melhoria em que devem ser fortalecidos para segurança e conformidade.
- 29) Concentrar esforços para ajudar a reduzir os riscos, melhorar os mecanismos de correção das vulnerabilidades exploradas, considerar outros elementos que possam aprimorar a segurança e aplicar conforme o necessário.

7. REQUISITOS LEGAIS E NORMATIVOS

7.1 Marco Civil da Internet

O Marco Civil da Internet é a Lei nº 12.965 de 23 de abril de 2014 que regula o uso da internet no Brasil estabelecendo diretrizes, princípios, garantias, direitos e deveres para este uso.

7.2 LGPD

Está em vigor no Brasil a Lei nº 13.709/2018, denominada de Lei Geral de Proteção de Dados Pessoais (LGPD), que visa proteger dados de pessoas naturais. Por isso, são necessários cuidados quando tratamos dados pessoais, que inclusive podem ser de natureza sensível. Algumas condutas são esperadas dos colaboradores:

- a) Se você não precisa de algum tipo de dado específico, não peça e não receba.
- b) Somos responsáveis pelos dados que nos são fornecidos.
- c) Evite imprimir dados pessoais, só faça se for realmente importante.
- d) Dissemine a nossa cultura de privacidade e proteção de dados pessoais.

Cada colaborador é responsável pelos dados que processa e deve, pessoalmente, ou com a ajuda do Comitê de Segurança e Privacidade da Informação, garantir sua segurança.

7.3 ISO/IEC 27001:2022

A ABNT NBR ISO/IEC 27001:2022 é uma norma que fornece os requisitos e diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação.

7.4 ISO/IEC 27701:2019 Versão corrigida 2020

A ABNT NBR ISO/IEC 27701:2019 é uma norma que fornece os requisitos e diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação na forma de uma extensão das ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022.

8. GLOSSÁRIO

Colaborador: um “Colaborador” é considerado qualquer pessoa, qualquer que seja seu status (diretor, funcionário, trabalhador temporário, trainee, estagiário, funcionário terceirizado etc.) que cria, consulta, utiliza e implementa recursos de TI.

Parceiros: Consultores, parceiros e funcionários de empresas prestadoras de serviços, os quais também deverão assinar um acordo atestando que respeitam as regras de utilização definidas neste documento.

Recursos de TI: são definidos como recursos que incluem sistemas de informática (principalmente programas, dados e servidores), equipamentos de informática (principalmente computadores e softwares) e meios de comunicação (sistemas de mensagens, acesso à internet, Intranet, telefones fixos e celulares etc.) disponíveis a qualquer colaborador do Grupo LUME.

Central de Serviços: departamento/área da empresa ou serviço de uma empresa que se responsabiliza por todos os equipamentos (estações de Trabalho, servidores, equipamentos de rede, armazenagem de dados, backup e sistemas de impressão etc.) e softwares de sistemas de informação, assim como a manutenção de serviços de telecomunicações.

POD: refere-se a "Personally Owned Device" (Dispositivo de Propriedade Pessoal). Este termo é usado para descrever dispositivos que pertencem aos indivíduos (como smartphones, tablets, laptops), mas que são utilizados para fins de trabalho ou acessam dados corporativos.

Informação Confidencial: refere-se a toda informação não-pública, qualquer que seja sua natureza, envolvendo o Grupo LUME e/ou um de seus colaboradores ou seus representantes legais, como informações técnicas, financeiras, estratégicas, comerciais, jurídicas ou “pessoais”, etc.

Comitê de Segurança e Privacidade: Comitê responsável por decisões e ações táticas no que concerne à segurança e privacidade da informação do grupo

LGPD (Lei Geral de Proteção de Dados Pessoais): Lei referente ao tratamento de dados pessoais.

ANPD (Autoridade Nacional de Proteção de Dados): órgão responsável por controlar a LGPD no Brasil.

Backup: serviço ou estrutura responsável por armazenar cópias de segurança do ambiente de TI.

Mídias Removíveis: qualquer equipamento que possa armazenar, transferir e/ou capturar dados e que possa se conectar a um computador, laptop ou nuvem, como por exemplo Pendrive, Celular, Laptop, Dispositivos de Backup etc.

CISO: chamamos de Chief Information Security Officer, o profissional responsável pelo controle e operação dos controles de segurança da informação, no que se refere à área de tecnologia da informação da empresa

DPO: chamamos de encarregado de dados ou Data Protection Officer (DPO) o profissional que, dentro de uma empresa, é encarregado por cuidar das questões referentes à proteção dos dados pessoais do GRUPO LUME e de seus clientes.

Dump: é um processo de salvar todas as informações contidas na memória do computador, isso permite uma análise de tudo o que estava ocorrendo no computador.

9. CONTROLE DE DOCUMENTO

Versão	Quando	Quem	O que	Aprovador	Validador
0.0	08/05/2023	Edson Gonçalves	Elaboração.	Comitê de Segurança e Proteção de Dados	Danielle Martins
1.0	29/06/2023	Edson Gonçalves	Adição de conteúdo.	Comitê de Segurança e Proteção de Dados	Danielle Martins
2.0	25/03/2025	Danielle Martins	Revisão do conteúdo	Comitê de Segurança e Proteção de Dados	Danielle Martins