ÍNDICE

1. Objetivo

O objetivo da Política de Utilização de Recursos é a definição dos controlos e normas a seguir pelos colaboradores e subcontratados do GRUPO PRECERAM e suas afiliadas, de modo a garantir um uso apropriado dos ativos e recursos profissionais que são colocados sob sua responsabilidade e/ou utilizados na execução das suas tarefas.

2. Definições

- Profissional – Que se relaciona com uma dada profissão.
- Recurso – Ativo ou grupo de ativos móveis ou imóveis e qualquer serviço, próprio, alugado ou subcontratado disponibilizado pelo Grupo Preceram e suas afiliadas (ex.: farda, armário, viatura, sala, computador, telemóvel, email).
- Utilizador – Colaborador ou subcontratado que utilize um recurso disponibilizado pelo Grupo Preceram e suas afiliadas.

3. Princípios

- Os meios de controlo devem obedecer aos princípios da necessidade, proporcionalidade e boa-fé, sendo o menos intrusivos possível, e satisfazendo os legítimos objetivos da empresa.
- O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.
- O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, ou seja, a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança, constitui um interesse legítimo do responsável pelo tratamento. Pode ser esse o caso quando o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas.
- A relação entre a tecnologia e o Direito está espelhada, de modo especial, na proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD), nas medidas adequadas para garantir a segurança do tratamento (artigo 32.º do RGPD), na notificação de violações de dados pessoais às autoridades de controlo (artigo 33.º do RGPD), na comunicação de violação de dados pessoais aos titulares dos dados (artigo 34.º do RGPD) e na avaliação de impacto sobre a proteção de dados (artigo 35.º do RGPD).

4. Responsabilidade e Utilização

Responsabilidades do utilizador

- O utilizador deve assegurar que a utilização que faz dos recursos que lhe foram disponibilizados pelo GRUPO PRECERAM é efetuada com observância da legislação em vigor e das políticas, regulamentos e procedimentos internos.

- O utilizador é responsável pelo uso, integridade e segurança dos recursos atribuídos, garantindo que não são utilizados para fins diferentes daqueles para os quais foram concebidos, configurados e/ou autorizados.
- Fica vedado ao utilizador a remoção, desconexão, substituição ou qualquer alteração das caraterísticas físicas ou técnicas dos recursos, sem o prévio consentimento escrito da área responsável pela gestão do recurso.
- O utilizador deve facilitar o acesso aos recursos pelo tempo necessário para a sua reparação e/ou para efetuar qualquer serviço de manutenção preventiva ou outra.
- O utilizador deve comunicar, com a maior brevidade possível, qualquer incidente (ex: avaria, dano, furto, etc.) que ocorra com os recursos que lhe foram disponibilizados pelo Grupo Preceram à informática interna. De forma a garantir que, em caso de utilização indevida, furto ou extravio de um recurso, o Grupo Preceram desencadeia procedimentos para cessar o acesso, eliminar os dados ou bloquear o seu normal funcionamento.

Utilização Aceitável

- É considerada uma utilização aceitável do recurso:
  - ✓ A utilização na execução das atividades necessárias ao desempenho das funções do utilizador;
  - ✓ No acesso à informação do GRUPO PRECERAM, para qual existe autorização.

Utilização Não Aceitável

- É considerado uso indevido e não permitido do recurso:
  - ✓ Utilização abusiva que prive ou limite o acesso ou a utilização normal do recurso, bem como, provoque custos excessivos não previstos ou não autorizados;
  - ✓ Utilização de recursos sem autorização prévia;
  - ✓ Uso para fins comerciais, publicitários e de divulgação em proveito do próprio utilizador ou de terceiros;
  - ✓ A divulgação ou o armazenamento de conteúdos escritos, imagens, vídeos ou outros tipos de conteúdos, considerados ilícitos, fraudulentos, obscenos ou pornográficos e que estejam em violação da legislação em vigor e/ou das políticas, regulamentos internos do GRUPO PRECERAM;
  - ✓ Se houver propósito de difamar, assediar ou caluniar indivíduos ou organizações, ou que seja interpretado ou considerado como comportamento abusivo, obsceno ou de difamação;
  - ✓ Qualquer outra utilização que resulte em incumprimento da legislação em vigor das políticas e/ou regulamentos internos do GRUPO PRECERAM.

5. Destinatários e Acesso à Informação

Destinatários
Administração (responsável pelo tratamento) Data Protection Officer (garantir os direitos e liberdades dos utilizadores) Administradores técnicos das aplicações (sob autorização) Legal (em caso de litígio)
Acesso à Informação
Os dados pessoais recolhidos não são objeto de qualquer análise, a menos que ocorram eventuais incidentes ou eventos de segurança ou privacidade, pedido judicial, de uma autoridade de controlo ou exercício dos direitos do titular dos dados ou defesa de um direito em processo judicial, onde seja necessária uma análise ao recurso em causa, sendo nesse caso os dados comunicados às autoridades e destinatários competentes. Considerando o tipo de informação recolhida e a utilização que lhe é dada, considera-se não haver risco de intrusão na privacidade dos utilizadores, pelo que não prevalecem os direitos e liberdades dos titulares dos dados, tal como exigível pela alínea f) do n.º 1 do artigo 6.º do RGPD.

6. Política de Utilização de Recursos, Política de Utilização de Logs e Registo de incidentes, falhas, eventos de segurança.

6.1 Logs

- Devem ser adotadas medidas que impeçam o acesso à informação por pessoas não autorizadas, estabelecendo-se um perfil de acesso específico aos registos de eventos.
- Tem de ser garantido um acesso restrito, sob o ponto de vista físico e lógico, aos servidores do sistema, os quais devem manter um registo de acesso à informação sensível para controlo das operações e para a realização de auditorias internas e externas.
- De forma a garantir a rastreabilidade dos acessos de monitorização é necessário observar a parametrização dos sistemas para que os logs registem quem fez o acesso, respetiva data e hora (timestamp), operações efetuadas atribuindo um número sequencial (id) a cada ocorrência e um campo de hash aplicado sobre os elementos anteriores (id, utilizador, data, hora e operação).
- Os logs não podem ser utilizados na aferição do desempenho profissional do colaborador. A segurança dos dados pessoais captados nos logs é assegurada através da encriptação sempre que possível, pelo tempo de retenção definido e controlo de acessos.
- Os *logs* e *audit* logs dos sistemas deverão ser protegidos contra destruição, adulteração e acesso não autorizado.

6.2 Encriptação – Política de Controlo Criptográfico

- Devem ser usados controlos criptográficos em todos os ativos de informação, nomeadamente nos dispositivos móveis incluindo os BYOD e nos discos rígidos dos portáteis bem como nos discos externos, caso não ponham em causa o desempenho da máquina ou a assistência ao cliente.
- Os computadores portáteis são obrigados a ter a autenticação multifator.
- Não é permitido aos colaboradores terem informação da organização guardada no computador, devendo a mesma ser armazenada nas respetivas pastas no servidor.
- Equipamentos que possuam alguma forma de armazenamento (exemplo: portáteis, smartphones, tablets, discos amovíveis, …) não podem transportar dados de clientes (exemplo: base de dados) nem dados pessoais (exemplo: dados de identificação) caso não tenham ativado um mecanismo de encriptação.
- O acesso a qualquer ativo criptográfico por parte de uma autoridade pública é possível através de mandato judicial.
- Informação criptográfica transferida para outro país tem de respeitar a sua legislação nacional.

6.3 Política de Utilização de Dispositivos Móveis

- O uso de dispositivos móveis com capacidade de email corporativo obriga aos utilizadores dos mesmos a aceitarem o seu controlo parcial por parte do **GRUPO PRECERAM**.
- As seguintes regras definem a Mobile Policy do **GRUPO PRECERAM**:
  - ✓ Obriga ao uso de PIN.
  - ✓ É permitido o uso das seguintes capacidades:
    - Wi-Fi
    - Partilha de internet a partir do dispositivo
    - *Remote Desktop*
    - *Browser*
- Nos dispositivos móveis, como os portáteis, serão instalados certificados digitais para poderem navegar na rede interna do **GRUPO PRECERAM.**

- O uso de telemóveis apenas será possível, usando uma rede específica designada GP, que permite apenas um acesso restrito à internet.
- Em caso de roubo e ou extravio do dispositivo o utilizador deve comunicar tal facto ao departamento de IT.
- Caso um colaborador cesse as suas funções do GRUPO PRECERAM, a conta de email dos equipamentos pessoais é inativada pelo departamento de IT.
- No final da sua vida útil deve-se apagar toda a informação contida no dispositivo móvel e realizar um restauro para a versão de fábrica seguindo as recomendações do documento de destruição de suportes amovíveis e da informação.

6.4 Utilização dos recursos da Organização

- Regra geral os utilizadores não podem utilizar as Tecnologias de Informação (TI) para assuntos não relacionados com o GRUPO PRECERAM ou seja, não profissionais; estando proibida a utilização pelos utilizadores dos equipamentos e dispositivos por esta disponibilizados, entre os quais, o computador, para fins pessoais, lúdicos, ilegais ou que violem os direitos de propriedade intelectual em sentido estrito (direitos de autor e direitos conexos) ou de propriedade industrial (nomeadamente, marcas e patentes).
- O grau de tolerância admitido na utilização para fins privados das tecnologias de informação e comunicação no contexto laboral disponibilizadas pelo do GRUPO PRECERAM só a título muito excecional e nos casos em que, a não utilização, imponha um alto risco para os direitos e liberdades do utilizador.
- As consequências da má utilização ou utilização indevida dos meios de comunicação e tecnologias de informação colocados à disposição do utilizador são ficar sujeito a procedimento disciplinar e a possíveis penalidades criminais e cíveis, no caso dos colaboradores, ou ficar sujeito a rescisão do contrato de prestação de serviços e a possíveis penalidades criminais e cíveis, no caso de serem comissionistas.
- Os Postos de trabalho podem sofrer auditorias efetuadas pela Informática Interna e em caso de identificação de software ou hardware não autorizado este poderá ser sujeito a processo de desinstalação sem aviso prévio ao utilizador.
- Os utilizadores não podem utilizar as TI para fins maliciosos (propagação de vírus, roubo de Informação, etc.).
- Os utilizadores devem evitar monopolizar as TI do GRUPO PRECERAM quer seja sobrecarregando a rede com quantidades excessivas de informação, desperdiçando espaço em disco, recursos da impressora, entre outros.
- Os utilizadores não podem ceder, emprestar ou vender acesso às TI da empresa.
- O uso dos recursos por indivíduos ou organizações exteriores requer a permissão da Direção/Departamento responsável e notificação ao Responsável pela Informática Interna ou ao DPO.
- As TI não podem ser utilizadas para tentar obter acesso a computadores ou sistemas confidenciais para os quais o utilizador não tenha acesso.
- Todo o utilizador que encontrar uma possível quebra de Segurança ou Privacidade em qualquer sistema informático deve relatá-la à Informática Interna.
- Os utilizadores não podem instalar software não autorizado, sendo da total responsabilidade do mesmo essa ação.

6.5 Utilização de correio eletrónico

- O GRUPO PRECERAM providencia o uso de um sistema de correio eletrónico para ajudar os utilizadores no desempenho do seu trabalho e o seu uso deverá ser limitado às atividades de âmbito profissional.
- O GRUPO PRECERAM rege-se pelo Artigo 22.º da Lei n.º 7/2009 de 12 de fevereiro – Código do Trabalho, no qual consta que "o trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou

consulte, nomeadamente através do correio eletrónico." O mesmo artigo também refere "o disposto no número anterior não prejudica o poder de o empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio eletrónico".

- O uso pessoal das coordenadas eletrónicas de contacto profissional, não é permitido pelo GRUPO PRECERAM. A título muito excecional caso haja a necessidade de envio de algum e-mail não profissional através da conta da empresa numa situação real de emergência em que não haja a possibilidade de se usar outro meio de comunicação o mesmo deve ser arquivado numa pasta com o nome PESSOAL e apagado no mais curto espaço de tempo possível. O e-mail da empresa constitui-se como uma ferramenta exclusiva de trabalho e a troca de e-mails apenas de natureza profissional. Deve ser muito limitada, residual mesmo, a sua utilização fora do âmbito da atividade da empresa.
- O uso pessoal nunca poderá afetar o fluxo de tráfego normal do correio eletrónico a nível empresarial. O GRUPO PRECERAM reserva o direito de remover o correio eletrónico pessoal identificável para preservar a integridade dos sistemas de correio eletrónico.
- É proibido o uso do e-mail corporativo como meio de divulgação de mensagens ofensivas (raça, cor, orientação sexual, etc.) assim como de envio de Informação não relacionada com a atividade da empresa (pornografia, vídeos, etc.).
- Não se pode usar o e-mail da empresa em registo de sites não profissionais como por exemplo redes sociais, blogs e lojas de comercio, onde não haja uma relação direta com as atividades desenvolvidas da organização.
- Não se podem configurar contas de e-mail pessoais no computador da empresa; apenas se devem configurar contas profissionais.
- O Grupo Preceram não aconselha, mas não impede, o acesso a caixas de correio pessoal via navegador da internet, browser, sem recurso a armazenamento local, através dos dispositivos da empresa. Esses acessos devem ser feitos, preferencialmente, fora do horário de trabalho e não usando o acesso corporativo da empresa, visto não ser tecnicamente possível, distinguir esse tráfego pessoal do profissional podendo o mesmo ser alvo de monitorização involuntária. O acesso via telemóvel usando os dados de internet do mesmo revela-se como a melhor opção, a mais segura, não sendo a mesma monitorizada.
- Não é permitido o uso do e-mail para envio de chain mails e joke e-mails. A utilização de e-mails massivos deve ser previamente aprovada, de modo que se avalie corretamente o motivo e o respetivo conteúdo do mesmo.
- A receção de e-mails com o mesmo teor do previamente referido, ou que representem um uso abusivo do serviço, deve ser denunciada à Informática Interna.
- Como medidas preventivas estão implementados mecanismos automáticos que permitem efetuar a filtragem deste tipo de e-mails diretamente no servidor, nomeadamente:
  - ✓ Eliminação ou quarentena de mensagens que detetem a utilização de termos não autorizados;
  - ✓ Eliminação de mensagens que contenham anexos não autorizados (ficheiros executáveis, macros, etc.);
  - ✓ Limitação do tamanho de mensagens a enviar e receber.
- O GRUPO PRECERAM por norma não acede ao conteúdo das mensagens a não ser por pedido judicial ou na prevenção ou deteção da divulgação de segredos comerciais quando existem fundadas suspeitas. Nestes casos o acesso é efetuado na presença do utilizador em questão e do DPO, se possível, e limitar-se-á à visualização dos endereços dos destinatários, o assunto, a data e hora do envio.
- Os utilizadores da empresa devem encontrar-se sensibilizados para estes aspetos e para o facto de existirem mecanismos de controlo automáticos realizados de forma aleatória.
- Não é permitida a utilização de serviços públicos de correio eletrónico (ex.: Hotmail, Gmail), para o envio de qualquer informação relativa e decorrente das atividades do GRUPO PRECERAM.

- Nos casos onde exista a necessidade da introdução da coordenada profissional em plataformas (e.g., compras) geridas pelo utilizador para a receção de alertas e outras informações, deve-se solicitar aos sistemas de informação um endereço genérico.
- Não é considerado aceitável, o envio de mensagens para listas de distribuição internas nas seguintes situações:
  - ✓ Divulgação de assuntos não relevantes ao funcionamento do GRUPO PRECERAM;
  - ✓ Mensagens de natureza pessoal;
  - ✓ Anúncios de natureza comercial e publicitários;
  - ✓ Quaisquer outras mensagens de conteúdo abusivo ou impróprio, que violem a legislação em vigor, a presente política e/ou demais políticas, regulamentos e/ou procedimentos internos em vigor no GRUPO PRECERAM.
- Delegação de acesso à caixa de correio de utilizadores: no caso de férias e de ausência prolongada a colocação da mensagem de ausência, *Out off office*, é obrigatória por parte do utilizador. Caso o mesmo não o faça, a informática interna acederá à caixa de correio profissional com o intuito exclusivo da colocação da dita mensagem.

6.6 Utilização da Internet

- O acesso à Internet através da rede corporativa é concedido a todos os utilizadores como uma ferramenta para o desempenho das suas funções profissionais.
- A ligação à Internet através da infraestrutura deve ter como objetivo o cumprimento das funções de cada colaborador, não podendo ser usada para fins lúdicos ou pessoais durante o horário de expediente.
- Entende-se ser admissível um certo grau de tolerância em relação ao acesso à Internet para fins privados, nomeadamente se este ocorrer fora do horário de trabalho e se o mesmo não puser em causa a qualidade do serviço prestado.
- Na realização de um acesso privado, fora do horário de trabalho, deve-se evitar a utilização de websites bancários, contas de email privadas e qualquer outro site onde seja necessário a introdução de credenciais. O acesso via telemóvel usando os dados de internet do mesmo, revela-se como a melhor opção e a mais segura, não sendo a mesma monitorizada.
- O acesso à Internet não pode ser usado para quaisquer fins que violem, ou tenha como objetivo violar, a lei vigente ou os direitos de propriedade intelectual de outrem.
- Qualquer irregularidade/anomalia detetada relativamente à Internet (interrupção do acesso, infeção por vírus, etc.) deve ser reportada à Informática Interna, que fará todas as diligências no sentido de normalizar o serviço.
- O GRUPO PRECERAM poderá bloquear o acesso a sites que considere desnecessários para o desempenho das funções dos seus utilizadores ou que possa considerar abusivos (por exemplo, sites com conteúdo pornográfico, racista, etc.), não significando que o facto de um determinado site não se encontrar bloqueado, seja por isso permitido.
- Não deve ser partilhada qualquer Informação relativa ou pertencente ao Grupo Preceram através da Internet, uma vez que esta ligação não oferece quaisquer mecanismos de segurança, exceto quando explicitamente indicado em contrário, ou quando esteja garantida a segurança da transmissão da Informação.
- O GRUPO PRECERAM monitoriza o acesso à Internet e guarda o registo de todas as atividades, de forma a poder detetar incumprimentos da política de acesso à Internet.
- O GRUPO PRECERAM não acede ao perfil pessoal do utilizador em redes sociais.
- Qualquer utilizador que desrespeite a política de acesso à Internet será alertado desse facto, podendo ser sancionado de acordo com a gravidade do seu ato. O utilizador tem o direito de acesso à prova recolhida.

6.7 Controlo de dados de comunicações telefónicas

- O número de telemóvel fornecido é concedido a todos os colaboradores como uma ferramenta para o desempenho das suas funções profissionais, passando-se o mesmo com os telefones fixos.
- Os contactos PESSOAIS não devem ser inseridos no cartão sim, micro sim, ou nano sim PROFISSIONAL.
- O GRUPO PRECERAM controla as chamadas efetuadas e recebidas através dos telemóveis dos utilizadores com plafond atribuído.
- O colaborador pode responder no tempo e local de trabalho a necessidades estritamente privadas, imperando o bom senso, usando o telemóvel atribuído.
- O GRUPO PRECERAM não tem acesso ao conteúdo, nem utiliza qualquer dispositivo de escuta, armazenamento, interceção e vigilância de comunicações.
- O GRUPO PRECERAM reserva o direito de barrar nos telemóveis e telefones fixos as chamadas de valor acrescentadas sendo esta medida generalizada a todos os dispositivos.
- Os equipamentos fornecidos de comunicação só devem conter na unidade de armazenamento dados profissionais.
- Os departamentos Financeiro e de Informática têm acesso às faturas de telecomunicações.

6.8 Gestão de Frota/Geolocalização

- Existem dispositivos de geolocalização nas viaturas pesadas disponibilizadas para o exercício da atividade profissional.
- Os dados pessoais decorrentes da utilização de dispositivos de geolocalização não são usados para controlo do desempenho do trabalhador nem para qualquer outra finalidade que não as mencionadas anteriormente.
- As viaturas pesadas com geolocalização não devem ser utilizadas para fins privados.
- No caso dos telemóveis e computadores portáteis, não são monitorizados a geolocalização dos equipamentos.
- O responsável pela logística, o responsável financeiro e o responsável pela informática têm acesso aos dados deste recurso.

Dados Recolhidos
(Gestão de Frota) Nome, Itinerário, dia, hora, kms, combustível, observações, matrícula (Geolocalização) Dados de geolocalização da viatura
Tempo de retenção
Dados de geolocalização da viatura um ano, outros dados dois anos.

6.9 Utilização de Ferramentas de Instant Messaging (Comunicações Unificadas)

- É permitida a utilização de programas de instant messaging/chat nos computadores do GRUPO PRECERAM. O GRUPO PRECERAM permite a todos os seus colaboradores a utilização do Microsoft Teams e o Whatsapp permitindo obter todas as vantagens desses programas, mas de uma forma segura e controlada.
- Não é permitida a criação e a utilização de contas individuais ou institucionais, em qualquer serviço público de comunicações unificadas (ex.: Facebook, Messenger), para efeitos profissionais e decorrentes das atividades utilizador, exceto quando expressamente autorizado pela Administração do GRUPO PRECERAM.
- Não é permitido o envio de qualquer informação relativa às atividades do GRUPO PRECERAM, através de contas de serviços públicos de comunicações unificadas (ex.: Facebook, Messenger) não oficiais e não autorizadas.

6.10 BYOD – Utilização de equipamentos pessoais no local de trabalho

- O GRUPO PRECERAM compreende que os colaboradores queiram trazer os seus equipamentos pessoais para o local de trabalho a fim de executarem parte das tarefas relacionadas com o expediente. Este fenómeno é conhecido como BYOD ou "*bring your own device*".
- O Grupo Preceram envidará todos os esforços em não processar qualquer tipo de informação do foro pessoal. Não é esse o seu intuito. Nesse sentido sempre que o dispositivo esteja ligado dentro do espaço físico do GRUPO PRECERAM ou remotamente via virtual *private network (VPN)* o utilizador deve apenas tratar de assuntos de carácter profissional.
- Se navegar na internet os sites visitados ficam registados na proteção de perímetro, vulgo firewall, sendo possível identificar o utilizador se e na medida o sistema de *intrusion prevention system* (IPS) detete um risco de segurança proveniente do dispositivo particular. Em nenhuma outra situação há verificação dos sites visitados por um utilizador em concreto a não ser por mandato judicial ou suspeitas fundamentadas de atividades ilícitas como downloads onde estejam a ser violados os direitos de autor ou atividades similares. O GRUPO PRECERAM aconselha a que use o plafond de dados ao navegar na internet não havendo, neste caso, qualquer monitorização.
- No caso de ser detetado um risco de segurança é possível a execução de um scan remoto de segurança para verificar riscos e vulnerabilidades, como por exemplo, malware. As pastas que são usadas, por princípio, apenas para fins privados como a de fotografias não são acedidas.
- Não é permitido guardar dados corporativos em dispositivos BYOD fora das instalações físicas da organização sem o mesmo estar cifrado e ter sido autorizado pela Administração. Os dados corporativos podem conter dados confidenciais ou dados pessoais de pessoas singulares afetas ou relacionados com a organização e a sua proteção é prioridade máxima para o GRUPO Preceram.

6.11 Câmaras de videovigilância (CCTV)

- Sistema dissuasor contra a violação do espaço físico do GRUPO PRECERAM.
- A informação é usada caso haja o registo de um evento de segurança ou privacidade, pedido judicial, de uma autoridade de controlo ou exercício dos direitos do titular dos dados ou defesa de um direito em processo judicial, onde seja necessária uma análise às imagens gravadas, para aferir a responsabilidade pela falta de algum ativo de informação, perceber eventuais intrusões existentes ou haja risco para os direitos e liberdades de terceiros.
- A colocação do sistema é feita em zonas de circulação de pessoas no edifício respeitando a legislação em vigor. Não são recolhidas imagens de acesso ao interior de instalações sanitárias, acesso e interiores de vestiários, áreas de descanso ou outras áreas destinadas aos trabalhadores, zonas de fabrico, zonas de espera, salas de reuniões e auditórios.
- Pretende-se com este tratamento assegurar a prevenção e dissuasão da prática de atos ilícitos, desempenhando a sua função de prossecução do interesse coletivo, na segurança da organização, colaboradores e visitantes do GRUPO PRECERAM.
- O tratamento dos dados visa exclusivamente a proteção de pessoas e bens.
- As imagens não servem para controlo do desempenho profissional dos colaboradores, nem as câmaras estão dirigidas sobre estes durante a atividade laboral.

Dados Recolhidos
Imagens captadas pelo sistema
Tempo de retenção
As imagens são retidas por 30 dias.

6.12 Controlos Biométricos

- O controlo de acessos e de assiduidade com recurso a dados biométricos apresenta-se como um meio adequado por corresponder a uma «finalidade legítima».
- Os dados biométricos serão obrigatoriamente eliminados no momento da transferência do colaborador para outro local de trabalho ou no caso da cessação do contrato de trabalho.
- Caso a utilização do sistema biométrico no âmbito da relação de trabalho levante dúvidas e receios o colaborador deve-as colocar ao DPO.
- O colaborador, em abstrato, pode opor-se ao tratamento sempre que hajam «razões ponderosas e legítimas relacionadas com a sua situação particular» e que se apresentem com relevância para fazer prevalecer o seu direito sobre os interesses do responsável pelo tratamento.
- A legitimidade para o tratamento de dados com a finalidade de controlo do horário de trabalho (assiduidade) tem como base legal a «prossecução de interesses legítimos do responsável».
- Os destinatários do tratamento da biometria são por norma o departamento de recursos humanos, podendo, no entanto, os dados serem visualizados por outras categorias de titulares como o responsável da informática interna, e o DPO em casos de eventos de segurança e privacidade, e pela Autoridade para as Condições do Trabalho (ACT).
- A utilização dos dados não envolve o controlo do desempenho profissional dos colaboradores.

Dados Recolhidos
(Horário) Data e hora de entrada / data e hora de saída O *template* da impressão digital e do reconhecimento facial, resultante de interpretação algorítmica de pontos fisiométricos, sem possibilidade de reconstrução do dado biométrico.
Tempo de retenção
Enquanto o colaborador exercer funções na organização.

6.13 Controlo de acessos físicos e lógicos

- Os acessos às instalações são controlados, sendo que algumas instalações do GRUPO PRECERAM deverão ser protegidas contra acessos não autorizados por meio de barreiras físicas tais como portas fechadas à chave e ferramentas de controlo de acessos.
- Todos os visitantes deverão ser registados à entrada das instalações e ser acompanhados durante toda a duração da sua visita.
- Todas as salas críticas, nomeadamente datacenters e onde se processem dados pessoais, deverão ser protegidas com ferramentas de controlo de acessos nomeadamente portas com recurso a chave.
- Os colaboradores não deverão deixar documentos confidenciais sobre as secretárias.
- O GRUPO PRECERAM deverá manter um registo, e.g., uma base de dados de utilizadores, onde se encontrem registados todos os colaboradores internos e externos, devendo conter informação relevante em termos de acessos lógicos e físicos aos ativos de informação aos quais tenham acesso, e.g., Identificador do utilizador (*username*); Nome do utilizador; Número de colaborador; Departamento; Função; Responsável hierárquico; Privilégios/Permissões de Acesso.
- A criação de contas de utilizadores deverá ter um processo associado de requisição, aprovação e registo e os direitos de acesso atribuídos devem assegurar que o utilizador apenas pode aceder à informação e sistemas para os quais foi estritamente autorizado.
- Os direitos de acesso à informação de cada utilizador são revistos sempre que houver alterações de funções tais como transferências, promoções, despromoções ou término de contrato, pelos responsáveis dos recursos/informação.

- Os acessos a sistemas e à informação autorizados para cada utilizador devem estar permanentemente atualizados e devem ser cancelados assim que estes cessem ou alterem as suas funções.
- As contas devem ser inequivocamente identificáveis utilizando o nome de utilizador associado.
- Os acessos aos sistemas deverão ser controlados por meios de identificação e de uma password, únicos para cada indivíduo, de modo a responsabilizá-lo pelas suas ações.
- Durante o login ou entrada em qualquer recurso ou ativo tecnológico se alguma parte dessa sequência de acesso estiver incorreta, o processo não deverá devolver qualquer indicação da origem do problema, devendo simplesmente informar que o processo de login está incorreto após a introdução de toda a informação.
- A ligação aos equipamentos deve ser suspensa - Session Time-out - caso haja não atividade superior a 10 minutos nos portáteis dos colaboradores e 10 minutos nos servidores e nos outros equipamentos de rede.
- A seleção de passwords é do critério do utilizador, estando este obrigado a seguir os standards estipulados de seguida. As passwords:
  - ✓ Não deverão conter parte ou na sua totalidade o username do utilizador;
  - ✓ Deverão conter caracteres de três das quatro categorias: maiúsculas (A – Z), minúsculas (a – z), numéricos (0 – 9) e não alfabéticos (~ ! @ # $ % & * ( ));
  - ✓ Deverão ter um comprimento mínimo de 8 caracteres para as estações de trabalho e 16 caracteres para os servidores e outros ativos de rede, e.g., firewalls e switches;
  - ✓ Deverão expirar após 365 dias;
  - ✓ Deve ser diferente da última;
  - ✓ Deverão ter uma duração mínima de 24h;
  - ✓ Deverão ser automaticamente desativadas após 5 tentativas falhadas de login.
- As passwords são confidenciais, pessoais e intransmissíveis pelo que não deverão ser escritas em locais visíveis e facilmente acessíveis. Igualmente estas não devem ser armazenadas em disco, smartphones ou dispositivos equivalentes, divulgadas por e-mail, ou por qualquer outra forma de comunicação eletrónica sem encriptação.
- Não devem ser utilizados mecanismos de login automáticos, onde não seja requerida a introdução de uma password.
- Em caso de suspeita de comprometimento de uma conta ou password, deve ser reportado o incidente para que se proceda de imediato à sua alteração.
- A password inicial de um utilizador só deve ser válida para efetuar o primeiro acesso. Nessa altura deve ser obrigatória e forçada a alteração da mesma.
- Sempre que um recurso tenha sido comprometido ou acedido indevidamente, o seu responsável deverá proceder de imediato à alteração de todas as passwords utilizadas no mesmo.
- A password inicial de um utilizador é transmitida verbalmente ao mesmo podendo a mesma também ser transmitida por SMS ou encriptada.

6.14 Utilização dos Postos de Trabalho

6.14.1 Antivírus

- Devem ser implementados mecanismos de prevenção que inviabilizem a contaminação dos equipamentos com software malicioso e, como complemento, devem ser implementados controlos que possibilitem a deteção e eliminação das referidas ameaças.
- O software antivírus deve encontrar-se permanentemente atualizado. As atualizações necessárias apenas devem ser retiradas do site do fornecedor do software.
- Todos os postos de trabalho devem conter software de antivírus e *anti-spyware* atualizado.

- Servidores de e-mail devem encontrar-se protegidos por software antivírus que suporte real-time *scanning* a *mailboxes*, e que analise a Informação que entre e saia, impedindo a propagação do mesmo para o destinatário, inviabilizando a propagação deste por desconhecimento do utilizador.
- Ficheiros ou macros provenientes de fontes desconhecidas ou não confiáveis não podem, em circunstância alguma, ser abertos.
- SPAM, chain mails e outros e-mails não relevantes para a atividade da empresa devem ser eliminados.
- O download de conteúdos deve ser restrito. Em particular, downloads de ficheiros executáveis devem ser restritos apenas a administradores de sistemas e caso seja essencial que estes o façam no âmbito da sua atividade. Não devem ser efetuados downloads de sites não confiáveis ou desconhecidos.

6.14.2 Clear Desk Policy

- Todos os dispositivos de armazenamento amovíveis que contenham material Confidencial devem ser guardados em local seguro quando não se encontram em uso.
- Informação de negócio confidencial deve ser guardada em armário fechado.
- Papeis e mídia digital que contenha informação relevante quando não em uso deve ser guardada em local apropriado como armários ou gavetas.
- Anotações, recados e lembretes não devem ser deixados visíveis na secretária, colados em paredes, divisórias ou no monitor do computador.
- Destruir os documentos impressos antes de os colocar no lixo. Utilizar as máquinas destruidoras para todos os documentos classificados como Confidencial.
- Informações sensíveis ou de risco para os direitos e liberdades dos titulares, se impressas, devem ser retiradas imediatamente do dispositivo de impressão.
- Não colocar recipientes com líquidos sobre a mesa e perto dos ativos de informação.
- No final do expediente e nos casos de ausência prolongada deve "limpar" a secretária através da arrumação de papéis, fecho das gavetas e armários e término da sessão de trabalho nos ativos de informação.

6.14.3 Clear Screen Policy

- Os ativos de informação como os computadores, terminais e impressoras, após um período de inatividade superior a 10 minutos são automaticamente alvos de uma política de ativação de *screen-saver* com recurso a password.

6.14.4 Acesso Remoto ao Computador ou dispositivo do Trabalhador

- O GRUPO PRECERAM não controla à distância a atividade do colaborador seja em tempo real, seja em tempo diferido através da gravação daquelas operações.
- As ferramentas utilizadas são a *remote desktop*, a assistência rápida da Microsoft, e a VNC.
- Não se recorre a sistemas que permitam a pesquisa, localização e obtenção de dados e informações eletrónicas (*Electronically Stored Information*), o que abrange todo o tipo de ficheiros e mensagens de correio eletrónico, nos computadores ou dispositivos da organização, exceto em caso de fundadas suspeitas, na procura de ficheiros maliciosos ou em caso de quebras ou fugas de segurança.
- De forma a garantir que não é acedida e copiada informação de natureza privada na realização de salvaguardas a mesma não é permitida nos computadores ou dispositivos da empresa, em especial, se tratar-se de informação que contenha Dados Pessoais de pessoas singulares. Apenas devem ser tratados assuntos de âmbito PROFISSIONAL nos computadores ou dispositivos facultados pelo GRUPO PRECERAM. Se por algum motivo de força maior e a título muito excecional o utilizador tenha de guardar informação pessoal num computador ou dispositivo da empresa a mesma deve ser arquivada dentro de uma pasta na raiz do dispositivo ou computador com o nome PESSOAL e retirada no mais curto espaço de tempo.

6.14.5 Impressoras

- As impressoras devem ser usadas para fins PROFISSIONAIS. Caso haja a necessidade pontual de imprimir um documento privado é possível, impera o bom senso, alertando-se para o facto do Grupo Preceram monitorizar a impressão.
- Os recursos de impressão como impressoras, fotocopiadoras, faxes e outros recursos com capacidade de reprodução ou de visualização de informação não devem ser deixados sem vigilância quando é impressa, ou está para ser impressa, informação sensível.

6.14.6 Software

- O não controlo da instalação de software pode levar a vulnerabilidades, divulgação de informação, perda de integridade e outro tipo de incidentes de segurança, bem como, a violação de propriedade intelectual.
- Nos dispositivos profissionais só se pode instalar software legal ou aprovado pelo GRUPO PRECERAM.
- As atualizações e os patches de segurança necessários ao correto funcionamento dos sistemas operativos e aplicações não carece de autorização desde que devidamente licenciados.
- Instalação de software para uso pessoal e software potencialmente malicioso ou suspeito não é permitido nos ativos de informação do Grupo Preceram.
- A instalação de software pelos utilizadores apenas é permitida caso os mesmos sejam necessários ao desempenho das suas funções profissionais. Apenas se devem descarregar e instalar software de repositórios fidedignos e assinados digitalmente.
- Utilizadores que pelo desempenho das suas funções sejam administradores locais das suas máquinas devem aplicar o princípio do menor privilégio na execução das aplicações e manter atualizado o seu computador ou dispositivo de trabalho.
- O GRUPO PRECERAM dispõe de ferramentas que alertam caso seja instalado software não autorizado e realiza varreduras de rede regularmente.

6.14.7 Aplicações

- O acesso a todas as aplicações é passível de ser alvo de monitorização, nomeadamente, atribuição de direitos de acesso e privilégio e garantir que os utilizadores fazem uma utilização correta dos dados.

6.15 Instrumentos de trabalho em ausências prolongadas e no término da relação laboral

- No caso de ausências prolongadas, superiores a trinta dias, em relação aos instrumentos de trabalho poderão ser efetuadas as operações seguintes:
  - ✓ A conta de utilizador ser desabilitada;
  - ✓ Ser solicitado a devolução dos instrumentos de trabalho (e.g., computador, telemóvel);
  - ✓ Na conta de correio eletrónico profissional deve ser colocada a mensagem de ausência e o ponto de contacto a partir do momento que a mesma não seja visualizada e tratada pelo colaborador.
- No término da relação laboral em relação aos instrumentos de trabalho são efetuadas as operações seguintes:
  - ✓ Correio eletrónico profissional – a coordenada eletrónica de contacto profissional é reencaminhada para o superior hierárquico ou colaborador do mesmo departamento, ou que desempenhe funções semelhantes, quando aplicável, pelo período de 1 ano após a qual é apagada. O colaborador deve apagar a pasta PESSOAL caso exista e informar, se aplicável, os contactos pessoais para não enviarem mais emails para o endereço em causa. Todos os restantes emails e arquivos profissionais não devem ser apagados e podem ser visionados caso haja algum assunto pendente com uma parte interessada

(e.g., cliente) cuja gravidade assim o justifique ou em caso de litigação. O tempo de retenção da caixa de correio eletrónico é analisado caso a caso e depende das funções e projetos nos quais o ex-colaborador esteve envolvido. Normalmente é eliminado de imediato (e.g., Consultores, Técnicos, Administrativos) podendo ser guardado até 1 ano em casos excecionais (e.g., Responsáveis de Área, Administradores).

- ✓ Dispositivo empresarial – o utilizador deve apagar, caso exista, a pasta PESSOAL do computador ou dispositivo empresarial. Não deve apagar os dados PROFISSIONAIS. Caso haja algum projeto a decorrer os dados PROFISSIONAIS podem ser acedidos e copiados a fim de permitir a execução do contrato com o cliente. O dispositivo ou computador é formatado de seguida.

- Número de telemóvel – o número PROFISSIONAL pode ser reencaminhado durante 1 mês caso as funções desempenhadas pelo colaborador que cessou as funções assim o exijam. Funções que exigem um reencaminhamento são as da área Comercial, Gestão de Clientes e Administração. O número não é eliminado, é desativado por um período de 3 meses, de forma que possa ser de novo atribuído a outro colaborador. Em casos excecionais e autorizados pela Administração, poderá o colaborador manter o seu contacto. Contactos pessoais que, excecionalmente, possam saber o número profissional devem ser informados a não realizarem mais chamadas.
- No caso de o colaborador não entregar algum ativo de informação, e.g., um equipamento, é possível que lhe seja imputado o custo do mesmo cabendo a decisão à direção à qual o colaborador está afeto em conjunto com a Administração.
- Instrumentos de trabalho adquiridos pelos colaboradores com capacidade de armazenamento são fornecidos sem sistema operativo e formatados.
- Ativos BYOD são verificados pelos sistemas de informação sendo garantido a eliminação de todos os dados empresariais, e.g., a conta de correio eletrónico corporativa no processo de término da relação contratual.
- Em todas as situações onde seja necessário aceder a um dispositivo de um ex-colaborador antes da sua formatação, o DPO é informado servindo de garante dos direitos de privacidade do mesmo.

6.16 Documentos Associados

- Política de Segurança