INFORMATION SECURITY MONITORING NOTICE - LATAM

Effective: 3rd April 2023

INTRODUCTION

The legal entity named on the contract of employment of the Employee, or the engagement of the Contractor (the "**Company**") has prepared this Information Security Monitoring Notice[1] (the "**Notice**") to supplement the Employee and Contractor Data Protection Notice (the "**DPN**") that you receive as an employee or contractor to set out its practices regarding the monitoring of data and other materials (including but not exclusively, business and personal[2] messages, communications and information) transmitted, received, processed and/or stored by the Company's electronic systems and devices. These include, but are not limited to, network, voice, computer, company issued mobile devices, instant messaging, web applications, mobile applications, social media, audio conferencing, video conferencing and fax infrastructure ("**Electronic Communications**"), printer use, the Internet, and physical access logs.

This Notice applies to all individuals or groups that have been provided with access to the Company's systems, facilities and/or information for a business purpose or supervisory function, including employees, consultants, contractors, non-executive directors and other workers in the Company (each an "**Authorized User**"). Appendix A sets out a non-exhaustive list of the communications and records which we monitor and from which we may collect any individually identifiable information on Authorized Users ("**Personal Data**") and the purposes for which we may use, transfer and disclose Personal Data.

In the event this Notice is provided to an Authorized User in a language other than English, any discrepancy, conflict or inconsistency between the two language versions shall be resolved as set out in the relevant DPN.

Irrespective of location, monitoring tools and processes are routinely deployed by the Company to the Company's electronic systems and devices to the extent not prohibited under local laws or regulations. All monitoring activity that takes place on the Company's electronic systems and devices is conducted in accordance with this Notice.

Any Personal Data collected in the course of the monitoring processes will be treated in accordance with the relevant DPN as issued from time to time. The processing of Personal Data is carried out with the aid of manual and electronic tools.

This Notice references key portions of relevant policies of the Company, but does not contain all of the Company's policies and requirements applicable to the use of Electronic Communications and the Internet. Authorized Users are required to comply with the requirements noted in the Company's Code of Conduct, Electronic Communications Guide and the Global Information Security Policy documents, as well as any other applicable standards issued by the Company from time to time. All capitalized terms used but not defined in this Notice shall have the meanings assigned to them in the Company's Global Information Security Policy documents.

Communications by certain regulated Company personnel are subject to additional detailed supervisory requirements and Authorized Users are reminded to consult the relevant policies and procedures for their

1 The Information Security Monitoring Notice (ISMN), was previously titled The Cyber Security Monitoring Notice (CSMN) and may also be referred to as such in other company documentation

2 In line with the Code of Conduct, authorized users are permitted limited personal use of company managed devices and applications, the internet and email for personal communications. The use of the resources may be monitored and inspected to maintain the integrity of the systems (e.g., monitoring for the introduction of malware or inappropriate data transmissions) and avoid activities that may give rise to company liability or risk.

line of business for further information.

All Electronic Communications, including emails (encrypted and unencrypted) and connections to the Internet and intranet websites using Company computing or network resources are the property of the Company and may be subject to monitoring and surveillance.

Subject to applicable law, this includes but is not limited to:

- **Conducting monitoring activities without giving prior notice ("covert monitoring"), in circumstances where it is permitted to do so (for example where it has suspicions of data exfiltration, criminal or other unlawful activities or breach of the Company's Compliance or Global Information Security Policies or breach of any other obligation owed to the Company);**
- **Monitoring and/or blocking of inbound and outbound emails and other messaging marked to indicate that they are personal or private or otherwise of a personal nature where it has a suspicion that such emails and their contents or attachments contravene or breach applicable law or Company's Compliance or Global Information Security Policies or any other obligation owed to the Company.**

PERSONAL DATA COLLECTION AND PURPOSES OF USE

Certain monitoring activities of the Company's electronic systems and devices are practiced throughout the Company for the purposes set out in Appendix A of this Notice.

The categories of Personal Data that the Company may process whilst undertaking the monitoring outlined in this Notice and the legal grounds for such processing (including consent, where necessary) are as set out in the relevant DPN.

SENSITIVE PERSONAL DATA

The Company may collect and process certain special categories of Personal Data including Sensitive Personal Data as set out in the relevant DPN in the course of conducting the activities described in this Notice.

Global Information Security monitoring activities do not actively monitor for Sensitive Personal Data, however some Sensitive Personal Data may inevitably be disclosed during monitoring for other types of data.

ACCESS BY COMPANY PERSONNEL

Access to Personal Data processed pursuant to this Notice is restricted to those individuals who need such access for the purposes listed in Appendix A. In addition to those individuals as set out in the relevant DPN, access will be granted on a strict need-to-know basis, to limited members of the Global Information Security Department and where necessary Internal Enterprise Investigations.

DISCLOSURE

The monitoring tools and processes described in this Notice may be deployed by the Global Information Security teams of the Company and any of its affiliates and branches including those located in the U.S., the U.K., Singapore, Hong Kong and India as well as within the specific country/region of operation. Personal Data may be stored in an Authorized Users home jurisdiction and/or other jurisdictions in which the Company has operations.

Given the global nature of the Company's activities, the Company may therefore transfer your Personal Data to countries located outside of your home country, as set out in the relevant DPN.

The Company may disclose, in accordance with applicable law, relevant Personal Data to any of its affiliates, and branches and they may process such Personal Data for the purposes set out in this Notice. In addition, the Company may disclose, in accordance with applicable law, relevant Personal Data to certain third parties as set out in relevant DPN.

SECURITY

The Company maintains appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of or damage to Personal Data.

MODALITIES OF THE PROCESSING AND DATA RETENTION

In processing Personal Data for the purposes set out in this Notice, the Company does not use automated decision making on Authorized User processes where the decision would have a legal or similarly significant effect on the authorized user when conducting monitoring as described in this Notice. 'Automated decision making' is the process of making a decision by automated means without any human involvement.

The retention periods for each type of data and jurisdiction are outlined on the Global Records Retention Schedule found on the Global Records Management page on Flagscape. Retention requirements are available upon request for new Authorized Users who do not yet have access to the internal site. The Company will delete Personal Data after the applicable retention period.

DISCIPLINARY ACTION

Authorized Users who violate any of the policies referenced in this Notice may be subject to investigation, suspension of access and/or disciplinary proceedings (up to and including termination of employment or contract services). Authorized Users who are not employees may be subject to referral to their employer for disciplinary action. Authorized Users who violate applicable laws or regulations may be referred to law enforcement and/or regulatory officials in accordance with legal and regulatory requirements. Any material or evidence identified via (including but not limited to) the monitoring of telephone calls, emails and Internet or intranet use (including personal telephone calls, emails and Internet usage) may be relied upon in any disciplinary proceedings and internal or external investigations. Authorized Users are expected to cooperate in inquiries, inspections, monitoring and recording activities if asked. Refusing to cooperate with a security investigation may result in legal or disciplinary action, including termination of employment or contract services.

CONTACT DETAILS

For questions or more information about this Notice or Global Information Security monitoring activities, Authorized Users should contact Global Information Security.

You may have the right to lodge a complaint with the Data Protection Authority for your country, for applicability and further information refer to the relevant DPN.

For questions regarding local laws and restrictions, Authorized Users should contact their local compliance officer, Data Protection Officer or legal department.

CHANGES TO THIS NOTICE

This Notice is not contractual and the Company reserves the right to modify or withdraw the Notice at any time. Should the Company make substantial changes to this Notice, it will notify Authorized Users as soon as reasonably possible by reissuing a revised Notice and/or taking other steps in accordance with applicable

laws.

Related Documents

Code of Conduct

Electronic Communications Retention – Enterprise Policy

Global Information Security Policy documents

Harassment & Discrimination Prevention – Enterprise Policy

Reputational Risk – Enterprise Policy

Violence Free Workplace – Enterprise Policy

Information Security Monitoring Notice - Flagscape

For additional policies, standards and guidelines, please see the Global Policy Source Flagscape page.

APPENDIX A

Refer to the matrix linked here to view the categories of data that may be collected for each purpose of use, summarized below. The matrix is available upon request for new Authorized Users who do not yet have access to the internal site.

The Communications and Records (both live and after the event) which we monitor on the Company's electronic systems and devices and from which we may collect Personal Data include, but are not limited to:

- Emails sent;
- Emails received;
- Web / internet usage, FTP, HTTP, HTTPS, Telnet;
- Print usage;
- Files located on desktop (outside My Documents), collaboration sites, open shares, internal Wiki's;
- Removable media, Non-Company managed devices connecting to Company system;
- Instant messaging;
- Telephone calls, VOIP calls, voicemails;
- Application access and usage logs and records;
- System access and usage logs and records (including records showing course of usage and conduct);
- Fax & Document Scanning/Imaging;
- Social media usage and content (external, non-Company);
- Open source and publicly available information;
- Security logs;
- Key logs and screen shots;
- Conferencing technologies;
- Cookies, Beacons, Sinkholes and Honeypots;
- GPS, Wi-Fi Tracking and Location Data;
- Swipe Card entry data;
- Text Messages sent and received.

The Purposes For Which We May Collect, Use, Transfer And Disclose Personal Data:

The Global Information Security Policy is designed to provide the necessary requirements to enable the Company to prepare, prevent, detect, respond and recover from increasing changes in the threat landscape. The Global Information Security Program provides solutions and uses advanced techniques to prevent information security threats from undermining customer confidence and disrupting business operations. Global Information Security protects the Company and its clients by using a risk-based and outcome-focused framework.

- Prepare: We protect by continually updating the Information Security Programme, which includes complying with local or foreign state and/or country specific laws to better anticipate and identify potential threats;

- Prevent: We protect by staying ahead of adversaries through the deployment of preventative controls to prevent loss, misuse and inappropriate use of confidential and proprietary information and reduce the number of incidents;
- Detect: We protect by limiting exposure through the deployment of detective controls including firewall monitoring, anti-spam and virus protection, and other monitoring; continuously monitoring all bank teammates, applications, data, systems and networks;
- Mitigate: We protect by mitigating incidents through an agile and coordinated response capability;
- Respond/Recover: We protect by improving security posture through robust forensics, investigations, and lessons learned capability while addressing any compliance issues, regulatory inquiries, disciplinary actions, or legal claims

AVISO DE MONITORAMENTO DE SEGURANÇA DAS INFORMAÇÕES - LATAM

Versão em português

Data de entrada em vigor: 3rd April 2023

INTRODUÇÃO

A pessoa jurídica indicada no contrato de trabalho do Funcionário ou a contratação do Prestador de Serviços (a "**Entidade**") preparou este Aviso de Monitoramento de Segurança da Informação[3] (o "**Aviso**") para complementar o Aviso de Proteção de Dados do Funcionário e do Prestador de Serviços (o "**DPN**") que você recebe como funcionário ou prestador de serviços para definir suas práticas relacionadas ao monitoramento de dados e outros materiais (incluindo, mas não exclusivamente, mensagens[4] pessoais e de negócios, comunicações e informações) transmitidos, recebidos, processados e/ou armazenados pelos sistemas e dispositivos eletrônicos da Entidade. Tais sistemas incluem, entre outros, infraestruturas de rede, voz, computadores, dispositivos móveis distribuídos pela Entidade, mensagens instantâneas, aplicativos da web, redes sociais, áudio conferência, videoconferência e fax (as "**Comunicações Eletrônicas**"), bem como registros de uso da impressora, de acesso à internet e acesso físico.

Este Aviso aplica-se a todas as pessoas ou grupos que receberam acesso aos sistemas, instalações e/ou informações da Entidade com objetivo de negócios ou função de supervisão, inclusive funcionários, consultores, terceirizados, diretores não executivos e outros colaboradores na Entidade (cada qual um "**Usuário Autorizado**"). O Anexo A estabelece uma lista incompleta das as comunicações e os registros que monitoramos e dos quais podemos coletar informações de identificação individual sobre usuários autorizados (os "**Dados Pessoais**"), bem como as finalidades com as quais podemos usar, transferir e divulgar Dados Pessoais.

Se este Aviso for apresentado ao Usuário Autorizado em um idioma que não seja o inglês, qualquer discrepância, conflito ou inconsistência entre as duas versões deverá ser resolvida conforme definido no DPN relevante.

Independentemente da localização, as ferramentas e processos de monitoramento são rotineiramente implantados pela Entidade nos sistemas e dispositivos eletrônicos da Entidade na medida em que não seja proibido pelas leis ou regulamentos locais. Toda atividade de monitoramento que ocorre nos sistemas e dispositivos eletrônicos da Entidade é conduzida de acordo com este Aviso.

Quaisquer Dados Pessoais coletados no decorrer dos processos de monitoramento serão tratados de acordo com o DPN relevante e conforme emitidos regularmente. O processamento de Dados Pessoais é realizado com o auxílio de ferramentas manuais e eletrônicas.

Este Aviso toma como referência partes essenciais de políticas relevantes da Entidade, mas não contém todas as políticas e requisitos da Entidade que são aplicáveis ao uso de comunicações eletrônicas e da internet. Os Usuários Autorizados devem cumprir os requisitos observados no Código de Conduta, no Guia de Comunicação Eletrônica e nos documentos da Política Global de Segurança da Informação da Entidade,

3 O Aviso de Monitoramento da Segurança da Informação (ISMN), anteriormente intitulado Aviso de Monitoramento da Segurança Cibernética (CSMN), também pode ser referido como tal em outra documentação da Entidade

4 De acordo com o Código de Conduta, usuários autorizados têm permissão de uso pessoal limitado dos dispositivos e aplicativos, internet e e-mail gerenciados pela Entidade para comunicações pessoais. O uso dos recursos pode ser monitorado e inspecionado, para manter a integridade dos sistemas (por exemplo, monitoramento contra a introdução de malware ou de transmissões indevidas de dados) e evitar atividades que possam dar origem à responsabilidade ou risco para a Entidade.

bem como qualquer outra norma aplicável emitida regularmente pela Entidade. Todos os termos em maiúsculas, mas não definidos neste Aviso, devem ser interpretados conforme os significados atribuídos a eles nos documentos da Política Global de Segurança da Informação da Entidade.

As comunicações por determinados funcionários regulados pela Entidade estão sujeitas a requisitos adicionais e detalhados de supervisão, e os Usuários Autorizados são instados a consultar as políticas e procedimentos relevantes para sua linha de negócios, para obter mais informações.

Todas as comunicações eletrônicas, inclusive e-mails (criptografados ou não) e conexões a sites de internet e intranet, que utilizam recursos de computação ou a rede da Entidade, são de propriedade da Entidade e podem estar sujeitas a monitoramento e vigilância.

Sujeito à lei aplicável, isso inclui, entre outros:

- **conduzir atividades de monitoramento sem aviso prévio ("monitoramento oculto"), em circunstâncias em que for permitido (por exemplo, quando houver suspeitas de vazamento de dados, atividades criminosas ou outras atividades ilegais, ou violações da Política de Conformidade ou da Política Global de Segurança da Informação da Entidade, ou violação de qualquer obrigação devida à Entidade);**
- **monitorar e/ou bloquear o envio e recebimento de e-mails e de outras mensagens identificadas como pessoais ou particulares, ou que tenham natureza pessoal de outra forma, quando houver suspeita de que o conteúdo ou anexos de tais e-mails violam ou desrespeitam a legislação aplicável, ou a Política de Conformidade ou a Política Global de Segurança da Informação da Entidade, ou qualquer outra obrigação devida à Entidade.**

COLETA DE DADOS PESSOAIS E OBJETIVOS DO USO

Certas atividades de monitoramento dos sistemas e dispositivos eletrônicos da Entidade são praticadas em toda a Entidade, para os fins estabelecidos no Anexo A deste Aviso.

As categorias de Dados Pessoais que a Entidade pode processar ao conduzir o monitoramento descrito neste Aviso e as bases legais para tal processamento (inclusive consentimento, quando necessário) são os estabelecidos no DPN relevante.

DADOS PESSOAIS CONFIDENCIAIS

A Entidade pode coletar e processar certas categorias especiais de Dados Pessoais, inclusive Dados Pessoais Sensíveis, conforme definido no DPN, no decorrer da realização das atividades descritas neste Aviso.

As atividades de monitoramento global de segurança da informação não monitoram ativamente os Dados Pessoais Sensíveis, mas alguns Dados Pessoais Sensíveis podem inevitavelmente ser divulgados durante o monitoramento de outros tipos de dados.

ACESSO PELO PESSOAL DA ENTIDADE

O acesso aos Dados Pessoais processados de acordo com este Aviso é restrito aos indivíduos que precisam de tal acesso para os fins listados no Anexo A. Além desses indivíduos, como estabelecido no DPN relevante, o acesso será concedido estritamente com base na necessidade de saber, para determinados membros do Departamento Global de Segurança da Informação e quando forem necessárias Investigações internas da Entidade.

DIVULGAÇÃO

As ferramentas e processos de monitoramento descritos neste Aviso podem ser implantados pelas equipes

de segurança da informação global da Entidade e suas afiliadas e agências, inclusive as localizadas nos Estados Unidos, Reino Unido, Singapura, Hong Kong e Índia, bem como dentro do país/região de operação específico. Os Dados Pessoais poderão ser armazenados na jurisdição na qual o Usuário Autorizado reside e/ou em outras jurisdições nas quais a Entidade opera.

Dada a natureza global das suas atividades, a Entidade pode, portanto, transferir seus Dados Pessoais para outros países além de seu país de origem, conforme estabelecido no DPN relevante.

A Entidade poderá divulgar, de acordo com a legislação aplicável, Dados Pessoais relevantes a qualquer uma de suas afiliadas e agências, que poderão processar tais Dados Pessoais para os fins estabelecidos neste Aviso. Além disso, a Entidade poderá divulgar, de acordo com a legislação aplicável, Dados Pessoais relevantes a determinados terceiros, conforme o DPN relevante.

SEGURANÇA

A Entidade mantém medidas organizacionais e técnicas adequadas para proteger contra o processamento não autorizado ou ilegal dos Dados Pessoais e/ou contra perda, alteração, divulgação ou acesso acidental, ou destruição ou danos acidentais ou ilegais aos Dados Pessoais.

MODALIDADES DE PROCESSAMENTO E PRESERVAÇÃO DE DADOS

Ao processar Dados Pessoais para os fins estabelecidos neste Aviso, a Entidade não usa a tomada de decisão automatizada nos processos do Usuário Autorizado nos quais a decisão teria um efeito legal ou similarmente significativo sobre o Usuário Autorizado, conforme descrito neste Aviso. “Tomada de decisão automatizada” é o processo de tomar uma decisão por meios automatizados sem qualquer envolvimento humano.

Os períodos de retenção para cada tipo de dados e jurisdição estão descritos no Cronograma Global de Retenção de Registros, encontrado na página Global Records Management no Flagscape. Os requisitos de retenção estão disponíveis mediante solicitação para Usuários Autorizados que ainda não têm acesso ao site interno. A Entidade excluirá os Dados Pessoais após o período de preservação aplicável.

AÇÃO DISCIPLINAR

Os Usuários Autorizados que violarem qualquer uma das políticas citadas neste Aviso podem estar sujeitos a investigação, suspensão de acesso e/ou processos disciplinares (até e inclusive a rescisão do contrato de trabalho). Os Usuários Autorizados que não forem funcionários podem estar sujeitos a encaminhamento para o seu empregador para ação disciplinar. Os Usuários Autorizados que violarem as normas e regulamentações aplicáveis poderão ser encaminhados a órgãos e/ou autoridades de ordem pública, de acordo com exigências regulatórias e legais. Qualquer material ou evidência identificada por meio de (entre outras medidas) monitoramento de chamadas telefônicas, e-mails e uso de internet ou intranet (inclusive chamadas telefônicas, e-mails e uso de internet para assuntos pessoais) podem ser invocados em qualquer processo disciplinar e investigações internas ou externas. Os Usuários Autorizados devem cooperar em consultas, inspeções, monitoramento e atividades de registro, caso seja solicitado. Recusar-se a cooperar com uma investigação de segurança pode resultar em ação legal ou disciplinar, incluindo a rescisão do contrato de trabalho ou serviços por contrato.

INFORMAÇÕES DE CONTATO

Em caso de dúvidas ou para obter mais informações sobre este Aviso ou sobre as atividades de monitoramento global de segurança da informação, os Usuários Autorizados devem entrar em contato pelo Segurança Global da Informação.

Você pode ter o direito de apresentar uma reclamação junto à Autoridade de Proteção de Dados do seu

país; para fins de aplicabilidade e para obter informações adicionais, consulte o DPN relevante.

Para questões sobre leis e restrições locais, os Usuários Autorizados devem entrar em contato com o diretor de conformidade, diretor de proteção de dados ou departamento jurídico local deles.

ALTERAÇÕES NESTE AVISO

Este Aviso não é contratual e a Entidade reserva-se o direito de modificar ou retirar o Aviso a qualquer momento. Caso a Entidade faça alterações substanciais a este Aviso, os Usuários Autorizados serão notificados assim que possível, reemitindo um Aviso revisado e/ou adotando outras medidas, de acordo com as normas aplicáveis.

Documentos relacionados

Código de Ética

Retenção de Comunicação Eletrônica — Política corporativa

Documentos da Política Global de Segurança da Informação

Prevenção de Assédio e Discriminação — Política corporativa

Risco à Reputação — Política corporativa

Local de Trabalho Livre de Violência — Política corporativa

Aviso de Monitoramento de Segurança da Informação — Flagscape

Para ler as políticas, normas e diretrizes adicionais, consulte a página Global Policy Source no Flagscape.

ANEXO A

Consulte a matriz vinculada aqui para visualizar as categorias de dados que podem ser coletados para cada finalidade de uso, resumidas abaixo. A matriz está disponível mediante solicitação para novos Usuários Autorizados que ainda não têm acesso ao site interno.

As Comunicações e os Registros (em tempo real e após o evento) que monitoramos nos sistemas e dispositivos eletrônicos da Entidade e dos quais podemos coletar Dados Pessoais incluem, entre outros:

- e-mails enviados;
- e-mails recebidos;
- uso de web/internet, FTP, HTTP, HTTPS, Telnet;
- uso de impressora;
- arquivos localizados na área de trabalho (externo a Meus Documentos), SharePoint, Discovery, Open shares e Wikis internos;
- mídias removíveis, dispositivos não gerenciados pela Entidade que se conectam ao sistema da Entidade;
- mensagem instantânea;
- chamadas telefônicas, chamadas por VOIP, correios de voz;
- registros de acesso e uso de aplicativos;
- registros de acesso e uso do sistema (inclusive registros que mostram o andamento do uso e a conduta);
- mensagens de fax e digitalizações/capturas de imagem de documentos;
- uso e conteúdo de redes sociais (externas, não pertencentes à Entidade);
- informações de código aberto e disponíveis publicamente;
- registros de segurança;
- registros de digitação e capturas de tela;
- tecnologias de conferência;
- cookies, beacons, sinkholes e honeypots;
- dados de localização, rastreamento por Wi-Fi e GPS;
- dados de entrada do cartão de acesso;
- mensagens de texto enviadas e recebidas.

Os fins para os quais coletamos, usamos, transferimos e divulgamos Dados Pessoais:

A Política Global de Segurança da Informação foi criada para fornecer os requisitos necessários para permitir que a Entidade se prepare, previna, detecte, responda e se recupere de mudanças crescentes no cenário de ameaças. O Programa Global de Segurança da Informação fornece soluções e utiliza técnicas avançadas para evitar que ameaças à segurança das informações prejudiquem a confiança do cliente e interrompam as operações comerciais. A Segurança Global da Informação protege a Entidade e seus clientes ao usar uma estrutura baseada em risco e focada em resultados.

- Preparar: Protegemos ao atualizar continuamente o Programa de Segurança da Informação, que inclui o cumprimento de leis locais ou estrangeiras estaduais e/ou nacionais específicas para melhor prever e identificar ameaças potenciais;

- Prevenir: Protegemos ao permanecermos à frente dos adversários por meio da implantação de controles preventivos para evitar perda, uso indevido e inadequado de informações confidenciais e proprietárias e reduzir o número de incidentes;
- Detectar: Protegemos ao limitar a exposição por meio da implantação de controles detetives, incluindo monitoramento de firewall, proteção antispam e antivírus e outros monitoramentos; monitorando continuamente todos os colaboradores, aplicativos, dados, sistemas e redes do banco;
- Diminuir: Protegemos ao mitigar incidentes por meio de uma capacidade de resposta ágil e coordenada;
- Responder/Recuperar: Protegemos ao melhorar a postura de segurança por meio de uma sólida capacidade forense, investigações e lições aprendidas, abordando quaisquer problemas de conformidade, consultas regulatórias, ações disciplinares ou reivindicações legais.

AVISO DE SUPERVISIÓN DE SEGURIDAD DE LA INFORMACIÓN - LATAM

Versión en español

Entrada en vigencia: 3rd April 2023

INTRODUCCIÓN

La entidad legal nombrada en el contrato de empleo del Empleado, o la contratación del Contratista (la "**Compañía**") ha preparado este Aviso de Supervisión de Seguridad de la Información[5] (el "**Aviso**") para complementar el Aviso de Protección de Datos del Empleado y Contratista (Data Protection Notice, "**DPN**") que usted recibe como empleado o contratista para establecer sus prácticas con respecto a la supervisión de datos y otros materiales (incluidos, entre otros, mensajes, comunicaciones e información comerciales[6] y personales) transmitidos, recibidos, procesados y/o almacenados por los sistemas y dispositivos electrónicos de la Compañía. Estos incluyen, entre otros, sistemas de red, de voz, computadoras, dispositivos móviles entregados por la compañía, mensajería instantánea, aplicaciones web, aplicaciones móviles, redes sociales, audioconferencias, videoconferencias e infraestructura de fax ("**Comunicaciones Electrónicas**"), el uso de impresoras, de Internet y registros de acceso físico.

Este Aviso rige para todas las personas o todos los grupos que cuenten con acceso a sistemas, instalaciones o información de la Compañía para un propósito comercial o una función de supervisión, que incluye empleados, consultores, contratistas, directores no ejecutivos y demás trabajadores en la Compañía (cada uno de ellos un "**Usuario Autorizado**"). El Apéndice A establece una lista no exhaustiva de las comunicaciones y los registros que supervisamos y de los cuales podemos obtener información que identifique personalmente a los Usuarios Autorizados ("**Datos Personales**") y los fines para los cuales podemos usar, transferir y divulgar Datos Personales.

En el caso de que el presente Aviso se proporcione a un Usuario Autorizado en un idioma distinto del inglés, cualquier discrepancia, conflicto o incoherencia entre las versiones en los dos idiomas se resolverá conforme a lo establecido en el DPN pertinente.

---

5 El Aviso de Supervisión de Seguridad de la Información (Information Security Monitoring Notice, ISMN), anteriormente se titulaba Notificación de Supervisión de Seguridad Informática (Cyber Security Monitoring Notice, CSMN) y es posible que también se haga referencia como tal en otra documentación de la Compañía

6 Conforme al Código de Conducta, los usuarios autorizados tienen permitido el uso personal limitado de dispositivos y aplicaciones administrados por la Compañía, Internet y correo electrónico para comunicaciones personales. El uso de los recursos puede supervisarse e inspeccionarse para mantener la integridad de los sistemas (p. ej., monitorear la introducción de malware o transmisiones de datos inapropiadas) y evitar actividades que puedan dar lugar a responsabilidad o riesgo de la Compañía.

Independientemente de la ubicación, la Compañía implementa de modo rutinario herramientas y procesos de supervisión en los sistemas y dispositivos electrónicos de la Compañía, en la medida en que no esté prohibido por las leyes o regulaciones locales. Toda actividad de supervisión que tenga lugar en los sistemas y dispositivos electrónicos de la Compañía se realiza de acuerdo con este Aviso.

Cualquier Dato Personal recopilado en el transcurso de los procesos de supervisión se tratará de acuerdo con el DPN pertinente y según se emita ocasionalmente. El procesamiento de los Datos Personales se lleva a cabo con la asistencia de herramientas manuales y electrónicas.

Este Aviso hace referencia a partes claves de las políticas relevantes de la Compañía, pero no contiene la totalidad de las políticas y los requisitos pertinentes de la Compañía en lo que respecta al uso de Comunicaciones Electrónicas e Internet. Se exige que los Usuarios Autorizados cumplan con los requisitos que se indican en el Código de Conducta, la Guía sobre Comunicaciones Electrónicas y la documentación de la Política de Seguridad de la Información Global de la Compañía, además de cualquier otro estándar correspondiente que la Compañía emita ocasionalmente. Todos los términos en mayúsculas que se usan pero no se definen en este Aviso tienen el significado que se les atribuye en la documentación de la Política de Seguridad de la Información Global de la Compañía.

Las comunicaciones realizadas por cierto personal regulado de la Compañía están sujetas a requisitos adicionales detallados de supervisión y se les recuerda a los Usuarios Autorizados que deben consultar los procedimientos y las políticas pertinentes para su línea de negocio para obtener mayor información.

Todas las Comunicaciones Electrónicas, incluidos los mensajes de correo electrónico (cifrados y no cifrados) y las conexiones a sitios de Internet y de la intranet mediante los recursos informáticos o de redes de la Compañía, son propiedad de la Compañía y pueden ser objeto de supervisión y vigilancia.

Sujeto a las leyes aplicables, esto incluye, entre otras tareas:

- **Realizar actividades de supervisión sin notificación previa ("supervisión encubierta"), en circunstancias que esté permitido hacerlo (por ejemplo cuando exista una sospecha de que se efectúan actividades delictivas u otro tipo de actividades ilícitas, o existe una violación de las Políticas de Cumplimiento o de Seguridad de la Información Global de la Compañía, o hay un incumplimiento de cualquier otra obligación para con la Compañía);**
- **Supervisar y/o bloquear los correos electrónicos entrantes y salientes, y otros mensajes marcados para indicar que son personales o privados, o de otro modo de naturaleza personal, en donde existe una sospecha de que dichos correos electrónicos y su contenido o archivos adjuntos infringen o violan las leyes aplicables o las Políticas de Cumplimiento o de Seguridad de la Información Global de la Compañía o de cualquier otra obligación para con la Compañía.**

OBTENCIÓN DE DATOS PERSONALES Y FINES DE UTILIZACIÓN

Determinadas actividades de supervisión de los sistemas y dispositivos electrónicos de la Compañía se realizan en toda la Compañía para los fines de establecidos en el Apéndice A de este Aviso.

Las categorías de Datos Personales que la Compañía puede procesar mientras lleva a cabo la supervisión detallada en este Aviso y los fundamentos legales para dicho procesamiento (incluido el consentimiento, en el caso que sea necesario) se rigen conforme a lo establecido en el DPN pertinente.

DATOS PERSONALES DE NATURALEZA SENSIBLE

La Compañía puede obtener y procesar determinadas categorías especiales de Datos Personales, incluidos los Datos Personales de Naturaleza Sensible, según se establece en el DPN pertinente, en el transcurso de las actividades descritas en este Aviso.

Las actividades de monitoreo de Seguridad de la Información Global no supervisan activamente los Datos Personales Confidenciales; sin embargo, ciertos Datos Personales Confidenciales pueden divulgarse inevitablemente durante la supervisión de otros tipos de datos.

ACCESO POR PARTE DEL PERSONAL DE LA COMPAÑÍA

Se restringe el acceso a los Datos Personales procesados conforme a este Aviso para aquellas personas que necesitan dicho acceso para los fines enumerados en el Apéndice A. Además de aquellas personas según se establece en el DPN pertinente, se permitirá el acceso limitado, cuando sea estrictamente necesario, a miembros del Departamento de Seguridad de la Información Global y en el caso de que sea necesario para Investigaciones Internas Empresariales.

DIVULGACIONES

Los procesos y las herramientas de supervisión descritas en este Aviso pueden ser implementados por los equipos de Seguridad de la Información Global de la Compañía y de cualquiera de sus afiliadas y sucursales, incluidas aquellas ubicadas en los Estados Unidos, el Reino Unido, Singapur, Hong Kong e India, así como también en el país/región específico en el que opere. Los Datos Personales se pueden almacenar en la jurisdicción local de los Usuarios Autorizados o en otras jurisdicciones en las que la Compañía lleve a cabo operaciones.

Dada la naturaleza global de las actividades de la Compañía, la Compañía puede entonces transferir sus Datos Personales a países ubicados fuera de su país de origen, según se establece en el DPN pertinente.

La Compañía puede divulgar, conforme a las leyes aplicables, Datos Personales pertinentes a cualquiera de sus filiales y sucursales, y pueden procesarse como Datos Personales para los fines establecidos en este Aviso. Además, la Compañía puede divulgar, conforme a las leyes aplicables, Datos Personales correspondientes a determinados terceros según se establece en el DPN pertinente.

SEGURIDAD

La Compañía aplica y mantiene medidas técnicas y organizativas oportunas para protegerse frente al tratamiento ilegal o no autorizado de los Datos Personales, o frente a cualquier pérdida, alteración, comunicación o acceso accidental, cualquier destrucción accidental o ilícita, o cualesquiera daños en los Datos Personales.

MODALIDADES DE PROCESAMIENTO Y RETENCIÓN DE DATOS

Al procesar Datos Personales para los fines establecidos en este Aviso, la Compañía no utiliza la toma de decisiones automatizadas en los procesos del Usuario Autorizado en los que la decisión tendría un efecto legal o similarmente significativo en el usuario autorizado al llevar a cabo la supervisión en la forma descrita en este Aviso. La “toma de decisiones automatizadas” es el proceso de tomar una decisión por medios automatizados sin ninguna participación humana.

Los períodos de retención para cada tipo de datos y jurisdicción se describen en el Programa global de retención de registros que se encuentra en la página Gestión Global de Registros en Flagscape. Los requisitos de retención se encuentran disponibles para los nuevos Usuarios Autorizados que todavía no tengan acceso al sitio interno, previa solicitud. La Compañía eliminará los Datos Personales después del período de retención correspondiente.

ACCIÓN DISCIPLINARIA

Los Usuarios Autorizados que violen cualquiera de las políticas mencionadas en el presente Aviso podrán ser

objeto de investigación, suspensión del acceso o procedimientos disciplinarios (que pueden incluir la terminación del empleo o de los servicios contratados). Los Usuarios Autorizados que no sean empleados podrán ser objeto de una remisión a sus empleadores para recibir medidas disciplinarias. Los Usuarios Autorizados que violen las leyes o reglamentaciones correspondientes podrán ser remitidos a las autoridades legales o los funcionarios regulatorios de conformidad con los requisitos legales y regulatorios. Podrá contarse con cualquier material o evidencia que se identifique mediante (incluyendo, a título enunciativo pero no limitativo) la supervisión de llamadas telefónicas, correos electrónicos y el uso de Internet o la intranet (incluso las llamadas telefónicas, mensajes de correo electrónico personales y el uso personal de Internet) en cualquier procedimiento disciplinario e investigación interna o externa. Se espera que los Usuarios Autorizados cooperen, en caso de que se les solicite, con las actividades de consulta, inspección, supervisión y registro. Negarse a cooperar con una investigación de seguridad puede tener como consecuencia una medida legal o disciplinaria, incluyendo la terminación del empleo o la rescisión de los servicios contratados.

DETALLES DE CONTACTO

Si tienen preguntas o para obtener más información acerca de este Aviso o las actividades de supervisión de la Seguridad de la Información Global, los Usuarios Autorizados deben comunicarse con Seguridad global de la información.

Es posible que tenga el derecho de presentar una queja ante la Autoridad de Protección de Datos de su país; para obtener información sobre la aplicabilidad y más información, consulte el DPN pertinente.

Para preguntas relacionadas con las leyes y restricciones locales, los Usuarios Autorizados deben comunicarse con el director de Cumplimiento, el director de Protección de Datos o el departamento Legal local.

CAMBIOS EN ESTE AVISO

Este Aviso no es un contrato y la Compañía se reserva el derecho a modificar o retirar el Aviso en cualquier momento. En caso de que la Compañía realice cambios sustanciales a este Aviso, notificará a los Usuarios Autorizados tan pronto como sea razonablemente posible volviendo a emitir un Aviso revisado o tomando otras medidas conforme a las leyes aplicables.

Documentos relacionados

Código de Conducta

Política Empresarial sobre la Retención de las Comunicaciones Electrónicas

Documentos de la Política Global de Seguridad de la Información

Política Empresarial sobre el Acoso y la Discriminación

Política Empresarial sobre el Riesgo para la Reputación

Política Empresarial sobre Lugar del Trabajo sin Violencia

Aviso de Supervisión de Seguridad de la Información en Flagscape

Para conocer las políticas, los estándares y las pautas adicionales, visite la página de la Fuente de Políticas Globales en Flagscape.

APÉNDICE A

Consulte la matriz vinculada aquí para ver las categorías de datos que pueden recopilarse para cada propósito de uso, resumidas a continuación. La matriz se encuentra disponible a solicitud para los Usuarios Autorizados que todavía no tengan acceso al sitio interno.

Las Comunicaciones y los Registros (en vivo y luego del evento) que supervisamos en los sistemas y dispositivos electrónicos de la Compañía y de los que podemos obtener Datos Personales incluyen, entre otros:

- correos electrónicos enviados;
- correos electrónicos recibidos;
- Uso de Internet, sitios web, FTP, HTTP, HTTPS, Telnet;
- uso de impresión;
- archivos ubicados en el escritorio (fuera de Mis documentos), sitios de colaboración, recursos compartidos abiertos, artículos de Wiki internos;
- Medios extraíbles, dispositivos no administrados por la Compañía que se conectan al sistema de la Compañía;
- Mensajería instantánea;
- Llamadas telefónicas, de VoIP, correos de voz;
- Registros e historiales de uso, y acceso de aplicaciones;
- Registros e historiales de uso, y acceso de sistemas (incluidos registros que muestran el curso del uso y comportamiento);
- Imagen/Escaneo de documentos y faxes;
- Uso y contenido de redes sociales (externas, que no pertenecen a la Compañía);
- Información disponible públicamente y de código abierto;
- Registros de seguridad;
- Capturas de pantalla y registros clave;
- Tecnologías de conferencias;
- Cookies, balizas electrónicas, sumideros de sistema de nombres de dominio y señuelos;
- GPS, Rastreo de Wifi y Datos de la Ubicación;
- Datos de ingreso en Lectores de Tarjetas;
- Mensajes de texto enviados y recibidos.

Fines para los que Podemos Obtener, Utilizar, Transferir y Divulgar Datos Personales:

La Política Global de Seguridad de la Información está diseñada para proporcionar los requisitos necesarios para permitir a la Compañía preparar, prevenir, detectar, responder y recuperarse de los cambios crecientes en el panorama de amenazas. El Programa Global de Seguridad de la Información proporciona soluciones y utiliza técnicas avanzadas para evitar que las amenazas a la seguridad de la información socaven la confianza del cliente e interrumpan las operaciones comerciales. Seguridad de la Información Global protege a la Compañía y a sus clientes mediante el uso de un marco basado en el riesgo y centrado en los resultados.

- Prepararse: protegemos al actualizar continuamente el Programa de Seguridad de la Información, que incluye cumplir con las leyes locales o extranjeras específicas del estado y/o país para anticipar e identificar mejor las posibles amenazas;
- Prevenir: protegemos al mantenernos por delante de los adversarios a través de la implementación de controles preventivos para evitar la pérdida, el uso indebido y el uso inapropiado de información confidencial y de propiedad exclusiva y reducir la cantidad de incidentes;
- Detectar: protegemos al limitar la exposición a través de la implementación de controles detectivos, incluida la supervisión de cortafuegos, la protección contra correo no deseado y virus, y otra supervisión; supervisamos continuamente a todos los compañeros de equipo, aplicaciones, datos, sistemas y redes del banco;
- Mitigar: protegemos mitigando incidentes a través de una capacidad de respuesta ágil y coordinada.
- Responder/recuperar: protegemos al mejorar la postura de seguridad a través de una sólida capacidad forense, de investigaciones y de lecciones aprendidas mientras abordamos cualquier problema de cumplimiento, consultas regulatorias, medidas disciplinarias o reclamaciones legales.