CORPORATE INFORMATION SECURITY POLICY

At METCOEX, information is a fundamental asset for the provision of its services and efficient decision-making, so there is an express commitment to protect its most significant properties as part of a strategy aimed at business continuity, the management of risks and the consolidation of a safety culture.

Aware of its current needs, METCOEX implements an Information Security Management System as the tool that identifies and minimizes the risks to which the information is exposed, establishes a security culture and guarantees compliance with legal and contractual requirements. current and other requirements of our customers and stakeholders.

As a key point of the policy is the implementation, operation and maintenance of an information security management system.

METCOEX Information Security Policy Fundamentals:

- Guarantee the confidentiality, integrity and availability of the information.
- Comply with all applicable legal requirements.
- Have a continuity plan that can recover from a disaster in the shortest time possible.
- Train and sensitize all employees on information security.
- Properly manage all incidents that occurred.
- All employees are informed of their security duties and obligations and are responsible for fulfilling them.
- Communicate mandatory compliance with this Policy to all METCOEX personnel and anyone working on their behalf, including contractors and visitors to our facilities.
- The System Manager is in charge of the Organization's Information Security Management System.
- Continuously improve the ISMS and, therefore, the organization's information security.

The objectives of this Policy will be:

a) Ensure that information assets receive an adequate level of protection.
b) Classify the information to indicate its sensitivity and criticism.
c) Define the levels of protection and special treatment measures according to their classification.

This Policy applies to all information managed in METCOEX, regardless of the support on which it is found.

The owners of the information are responsible for classifying it according to its degree of sensitivity and criticality, documenting and keeping the classification carried out updated, and defining the functions that must have access to the information.
The System Manager is responsible for ensuring that the security requirements established according to the criticality of the information they process are considered for the use of information technology resources.

Each Information Owner will supervise that the information classification and labeling process in their department is completed in accordance with the provisions of this Policy.

HUMAN RESOURCES SECURITY

The objectives of controlling the safety of personnel are:

- Reduce the risks of human error, start-up of irregularities, improper use of facilities and resources, and unauthorized handling of information.
- Explain the security responsibilities in the personnel recruitment stage and include them in the agreements to be signed and verify their fulfillment during the performance of the employee's tasks.
- Ensure that users are aware of information security threats and concerns and are trained to support the Company's Information Security Policy in the course of their normal duties.
- Establish confidentiality commitments with all personnel and users outside the information processing facilities.
- Establish the tools and mechanisms necessary to promote communication of existing security weaknesses, as well as incidents, in order to minimize their effects and prevent their recurrence.

This Policy applies to all Company personnel and external personnel who perform tasks within the Company.

The Human Resources Department will include information security functions in employee job descriptions, will inform all contracting personnel of their obligations regarding compliance with the Information Security Policy, will manage Confidentiality Commitments with staff and will coordinate user training tasks regarding this Policy.

The Information System Manager is responsible for monitoring, documenting and analyzing reported security incidents, as well as communicating them to the Information Security Committee and information owners.

The Information Security Committee will be responsible for implementing the means and channels necessary for the Information System Manager to handle reports of incidents and system anomalies. The Committee will also be aware, supervise the investigation, supervise the evolution of the information and promote the resolution of information security incidents.

The System Manager will participate in the preparation of the Confidentiality Commitment that will be signed by employees and third parties who perform functions in the Company, in advising on the sanctions that will be applied for breach of this Policy and in the treatment of information security incidents. .

All company personnel are responsible for reporting information security weaknesses and incidents that are detected in a timely manner.

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

The objectives of this policy are:

a) Prevent and prevent unauthorized access, damage and interference to the Company's headquarters, facilities and information.

b) Protect the critical information processing equipment of the Company, placing it in protected areas and protected by a defined security perimeter, with adequate security measures and access controls. Likewise, consider the protection of the same in its transfer and remain outside the protected areas, for maintenance or other reasons.

c) Control environmental factors that could impair the proper functioning of the computer equipment that houses the Company's information.

d) Implement measures to protect the information handled by the staff in the offices, within the normal framework of their usual tasks.

e) Provide protection proportional to the risks identified.

This Policy applies to all physical resources related to the Company's information systems: facilities, equipment, cabling, files, storage media, etc.

The Head of the Information System, together with the Information Holders, as appropriate, will define the physical and environmental security measures for the protection of critical assets, based on a risk analysis, and will supervise their application. It will also verify compliance with the physical and environmental security provisions.

The heads of the different departments will define the levels of physical access of the Company's personnel to the restricted areas under their responsibility. Information Owners will formally authorize off-site work with information about their business to Company employees when deemed appropriate.

All company personnel are responsible for compliance with the clean screen and desk policy, for the protection of information related to daily work in the offices.

ACCESS CONTROL POLICY TO INFORMATION SYSTEMS

The purpose of controlling access to information systems is:

a) Prevent unauthorized access to information systems, databases and information services.

b) Implement security in user access through authentication and authorization techniques.

c) Control security in the connection between the Company's network and other public or private networks.

d) Record and review critical events and activities carried out by users in the systems.

e) Raise awareness about their responsibility for the use of passwords and equipment.

f) Guarantee information security when using laptops and personal computers for remote work.

SYSTEM DEVELOPMENT AND MAINTENANCE POLICY

Security in the development and maintenance of systems aims to:

- Guarantee the inclusion of security controls and data validation in the development of computer systems.
- Define and document the standards and procedures that will be applied throughout the application lifecycle and in the base infrastructure on which they are supported.
- Define methods to protect critical or sensitive information.

This Policy applies to all computer systems, both self-developed or by third parties, as well as to all Operating Systems and / or Software that make up any of the environments managed by the Company.

The System Manager together with the owner of the Information will define the controls to be implemented in systems developed internally or by third parties, based on a prior risk assessment.

The System Manager, together with the Information Owner, will define, based on the criticality of the information, the requirements for protection by cryptographic methods. The person in charge of the information system will then define, together with the technical director of the department, the encryption methods to be used.

BUSINESS CONTINUITY MANAGEMENT POLICY

The security in the administration of the continuity of the activities of the company has as objectives:

a) Minimize the effects of possible interruptions to the normal activities of the Company (whether resulting from natural disasters, accidents, equipment failures, deliberate actions or other events) and protect critical processes through a combination of preventive controls and actions recovery.

b) Analyze the consequences of the interruption of the service and take the appropriate measures to prevent similar events in the future.

c) Maximize the effectiveness of the Company's contingency operations by establishing plans that include at least the following steps:

   1. Notification / Activation: Consisting of the detection and determination of damage and activation of the plan.
   2. Resume: Consisting of the temporary restoration of operations and recovery of the damage caused to the original system.
   3. Recovery: Consisting of restoring the capabilities of the system process to normal operating conditions.

d) Ensure coordination with Company personnel and external contacts who will participate in contingency planning strategies. Assign roles for each defined activity.

The System Manager will actively participate in the definition, documentation, testing and updating of contingency plans. The Information Owners and the System Manager will perform the following functions:

- Identify the threats that may cause interruptions in the processes or activities of the Company.
- Assess risks to determine the impact of such disruptions.
- Identify preventive controls.
- Develop a strategic plan to determine the global approach to address the continuity of the Company's activities.
- Prepare the contingency plans necessary to ensure the continuity of the Company's activities.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN CORPORATIVA

En METCOEX, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, por lo que existe un compromiso expreso de proteger sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la gestión de riesgos y la consolidación de una cultura de seguridad.

Consciente de sus necesidades actuales, METCOEX implementa un Sistema de Gestión de la Seguridad de la Información como la herramienta que identifica y minimiza los riesgos a los que se expone la información, establece una cultura de seguridad y garantiza el cumplimiento de los requisitos legales y contractuales actuales y otros requisitos de nuestros clientes y partes interesadas.

Como punto clave de la política es la implementación, operación y mantenimiento de un sistema de gestión de seguridad de la información.

Fundamentos de la Política de Seguridad de la Información de METCOEX:

- Garantizar la confidencialidad, integridad y disponibilidad de la información.
- Cumplir con todos los requisitos legales aplicables.
- Tener un plan de continuidad que pueda recuperarse de un desastre en el menor tiempo posible.
- Formar y sensibilizar a todos los empleados en seguridad de la información.
- Gestionar correctamente todos los incidentes que se produjeron.
- Todos los empleados son informados de sus deberes y obligaciones de seguridad y son responsables de cumplirlas.
- Comunicar a todo el personal de METCOEX y a cualquier persona que trabaje en su nombre el cumplimiento obligatorio de esta Política, incluidos los contratistas y visitantes de nuestras instalaciones.
- El Responsable del Sistema se hace cargo del Sistema de Gestión de Seguridad de la Información de la Organización.
- Mejorar continuamente el SGSI y, por lo tanto, la seguridad de la información de la organización.

Los objetivos de esta Política serán:

a) Asegurar que los activos de información reciban un nivel adecuado de protección.
b) Clasificar la información para indicar su sensibilidad y crítica.
c) Definir los niveles de protección y las medidas especiales de tratamiento según su clasificación.

Esta Política se aplica a toda la información gestionada en METCOEX, sea cual sea el apoyo en el que se encuentra.

Los propietarios de la información son responsables de clasificarla según su grado de sensibilidad y criticidad, documentar y mantener actualizada la clasificación realizada, y definir las funciones que deben tener permisos de acceso a la información.

El Responsable del Sistema es responsable de garantizar que los requisitos de seguridad establecidos de acuerdo con la criticidad de la información que procesan se consideren para el uso de los recursos de tecnología de la información.

Cada Propietario de la Información supervisará que el proceso de clasificación y etiquetado de la información en su departamento se complete de acuerdo con las disposiciones de esta Política

SEGURIDAD DE LOS RECURSOS HUMANOS

Los objetivos de controlar la seguridad del personal son:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Asegúrese de que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la Política de Seguridad de la Información de la Compañía en el curso de sus tareas normales.
- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal de la Compañía y el personal externo que realiza tareas dentro de la Compañía.

El Departamento de Recursos Humanos incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados, informará a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

El Responsable del Sistema de Información es responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarlos al Comité de Seguridad de la Información y a los propietarios de información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable del Sistema de Información maneje informes de incidentes y anomalías del sistema. El Comité también estará al tanto, supervisará la investigación, supervisará la evolución de la información y promoverá la resolución de incidentes de seguridad de la información.

El Responsable del Sistema participará en la preparación del Compromiso de Confidencialidad que firmará los empleados y terceros que desempeñen funciones en la Compañía, en el asesoramiento sobre las sanciones que se aplicarán por incumplimiento de esta Política y en el tratamiento de incidentes de seguridad de la información.

Todo el personal de la empresa es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente.

POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL

Los objetivos de esta política son:

a) Prevenir y prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de la Compañía.
b) Proteger el equipo de procesamiento de información crítico de la Compañía, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de la misma en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
c) Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de la Compañía.
d) Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
e) Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de la Compañía: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El Responsable del Sistema de Información, junto con los Titulares de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de la Compañía a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de la Compañía cuando lo consideren apropiado.

Todo el personal de la empresa es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

POLÍTICA DE CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

El control del acceso a los sistemas de información tiene por objeto:

a) Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.

b) Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.

c) Controlar la seguridad en la conexión entre la red de la Compañía y otras redes públicas o privadas.

d) Grabar y revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.

e) Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.

f) Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

POLÍTICA DE DESARROLLO Y MANTENIMIENTO DEL SISTEMA

La seguridad en el desarrollo y mantenimiento de sistemas tiene como objetivo:

- Garantizar la inclusión de controles de seguridad y validación de datos en el desarrollo de sistemas informáticos.
- Definir y documentar los estándares y procedimientos que se aplicarán durante el ciclo de vida de la aplicación y en la infraestructura base en la que se admiten.
- Definir métodos para proteger la información crítica o sensible.

Esta Política se aplica a todos los sistemas informáticos, tanto de desarrollo propio o de terceros, como a todos los Sistemas Operativos y/o Software que integren cualquiera de los entornos administrados por la Compañía.

El Responsable del Sistema junto con el propietario de la Información definirá los controles a implementar en sistemas desarrollados internamente o por terceros, sobre la base de una evaluación previa del riesgo.

El Responsable del Sistema junto con el Propietario de la Información, definirá en función de la criticidad de la información, los requisitos de protección por métodos criptográficos. A continuación, el Responsable del Sistema de información definirá, junto con el director técnico del departamento, los métodos de cifrado que se utilizarán.

POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La seguridad en la administración de la continuidad de las actividades de la empresa tiene como objetivos:

a) Minimizar los efectos de posibles interrupciones de las actividades normales de la Compañía (ya sean resultado de desastres naturales, accidentes, fallas de equipos, acciones deliberadas u otros hechos) y proteger los procesos críticos a través de una combinación de controles preventivos y acciones de recuperación.

b) Analizar las consecuencias de la interrupción del servicio y tomar las medidas adecuadas para prevenir hechos similares en el futuro.

c) Maximizar la efectividad de las operaciones de contingencia de la Compañía con el establecimiento de planes que incluyan al menos los siguientes pasos:

1. Notificación/Activación: Consistente en la detección y determinación de daños y activación del plan.
2. Reanudar: Consistente en la restauración temporal de las operaciones y la recuperación de los daños causados al sistema original.
3. Recuperación: Consistente en la restauración de las capacidades del proceso del sistema a condiciones normales de funcionamiento.

d) Garantizar la coordinación con el personal de la Compañía y los contactos externos que participarán en estrategias de planificación de contingencias. Asigne funciones para cada actividad definida.

El Responsable del Sistema participará activamente en la definición, documentación, pruebas y actualización de planes de contingencia. Los Propietarios de Información y el Responsable del Sistema realizarán las siguientes funciones:

- Identificar las amenazas que puedan causar interrupciones en los procesos o actividades de la Compañía.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global para abordar la continuidad de las actividades de la Compañía.

Preparar los planes de contingencia necesarios para asegurar la continuidad de las actividades de la Compañía.