1.0 OBJETIVO

Establecer normas que deben adoptarse para la Gestión y Control de la confidencialidad con el fin de proteger los intereses de la sociedad mediante la protección y la prevención de fuga o la divulgación de la información confidencial y los elementos que pueden afectar a **KOYO LATIN AMERICA.**

2.0 CAMPO DE APLICACIÓN

Todas las áreas de **KOYO LATIN AMERICA** de Panamá (en adelante KLA); empresa dedicada al Comercio y Distribución de Rodamientos y Productos Koyo.

3.0 DEFINICIONES

Los artículos incluyen información confidencial generada por **KLA** relacionados con las actividades comerciales, de investigación, desarrollo, producción, Recursos Humanos, Contabilidad y Finanzas, Legal, etc. que no se considera información pública.

También incluye toda la información que pueda ser perjudicial para **KLA** o sus socios comerciales que es utilizada por otros de manera inadecuada.

4.0 DOCUMENTOS ASOCIADOS

No se aplica.

5.0 RESPONSABILIDAD Y AUTORIDAD

Actividades	**Responsables**
Revisar y Aprobar las Políticas de Seguridad de la Información.	Presidente / Gte. Senior Oper.
Controlar el manejo de la Seguridad de Información por Departamento	Comité para el Control de la Información Confidencial
Promover y monitorear la ejecución de la Política de Confidencialidad.	Coordinadora de Gobierno Corporativo
Coordinar reuniones con la Gerencia para evaluar cambios a la Política o violaciones reportadas.	

6.0 SISTEMÁTICA

Clasificación de las Informaciones Confidenciales

Los elementos sensibles se clasifican de acuerdo a su importancia y a la norma descrita a continuación.

1. **Top Secret**
   "Top Secret" son todos los elementos sensibles basados en la Gestión Operativa de **KLA**, que cuando se divulgan indebidamente, pueden causar una pérdida muy severa, pérdida o daño a la sociedad, sus accionistas, afiliados y socios comerciales (proveedores y clientes).

   Los ítems clasificados como "**Top Secret**" no será revelada a ninguna persona que no sean los específicamente designados y autorizados por la empresa.
2. **Secret**
   "Secret" son todos los productos sensibles que no están clasificados como "Top Secret", pero pueden causar, si no están bien descritos, daños, pérdidas o daños a la empresa, sus accionistas, a los afiliados o sus parejas de negocio (clientes y proveedores).

   Los ítems clasificados como **Secret** no deben ser revelados a ninguna persona que no sean los específicamente designados y autorizados por la empresa.

3. **Restringido**
   "Restringido" son todos los elementos sensibles restringidos a las personas involucradas que no están clasificados como **Top Secret** o **Secret**, pero no deben ser revelados a cualquier persona que no este designada y autorizada por la empresa.

4. **Uso Interno**
   "Uso Interno" son todos los elementos que pueden ser consultados o utilizados por el personal de KLA. No están clasificados como **Top Secret**, **Secret** o **Restringido,** pero no deben ser revelados a cualquier persona que no forme parte de la empresa.

5. **Público**
   "Público" son todos los elementos no restringidos que pueden ser consultados por cualquier persona. No están clasificados como **Top Secret, Secret**, **Restringido** o **Uso interno**.

Clasificación de las áreas

Todas las dependencias del edificio de **KLA** se clasifican de acuerdo con su importancia y sus normas, se definen como se describe a continuación.

Zona C

Las áreas comunes de la compañía, tales como aparcamientos, espacios abiertos y espacios públicos que no tienen nada confidencial.

Zona B
Son las áreas de negocio que tienen elementos sensibles (por ejemplo, la construcción de la fábrica, la oficina, etc.)

Zona A
Estas son áreas que se incluyen en la Zona B y poseen información confidencial, por ejemplo, el análisis y las actividades de desarrollo, información técnica, diseño y planos, las especificaciones técnicas así como la información empresarial de los asociados.

Determinación del Responsable por el Control Confidencial

El Director de **KLA** debe determinar una persona que será la responsable de coordinar todos los asuntos relacionados con el control de la información confidencial de la empresa.

Tratamientos de la Información Confidencial:

La persona responsable del Control Confidencial debe definir los niveles de confidencialidad de cada ítem de Información Confidencial.

Esta definición se hará en conjunto con los jefes de departamento con el fin de controlar la confidencialidad de toda la organización, se cumplirá de acuerdo con las siguientes condiciones:

Declaración y Preparación

Cuando se crea una información considerada confidencial o cuando una persona tiene un contacto con información confidencial, esta persona debe informar a la persona responsable de la empresa del *control confidencial* para definir cuál es la clasificación adecuada de la confidencialidad.

Toda información externa debe ser presentada a la persona encargada del *control confidencial* para que esta determine el grado de confidencialidad de la misma.

Todo cuidado es necesario con el fin de minimizar los riesgos de que cualquier información, incluyendo un memo o un proyecto sea indebidamente divulgado y conocido por otros.

Marcación y Registro

Los elementos Confidenciales deberán ser marcados con una señal roja de la siguiente manera:

T **: Top Secret**

: Secret

: Restringido a las personas autorizadas

Cualquier información clasificada como **"Top Secret"** debe ser registrada y archivada en una lista de informaciones confidenciales. Esta lista debe ser implementada, actualizada y conservada por la persona responsable de controlar las confidencialidades.
La lista debe ser revisada y actualizada periódicamente, para asegurar que las informaciones obsoletas o innecesarias puedan ser eliminadas o modificadas.

Las copias deben ser identificados por un número de secuencia, cada número correspondiente a la copia del destinatario.

Los elementos cuya confidencialidad sea reducida o eliminada con el pasar del tiempo deben ser revisados para cambiar su nivel de confidencialidad.

Copia y Distribución

La información confidencial no puede ser copiada, sólo excepcionalmente, cuando sea absolutamente necesario por razones de negociación comercial.

En concreto, la información clasificada como **"Top Secret"**, Está prohibida la copia, reproducción o transferencia ya sea física o electrónicamente (incluyendo, fax, correo electrónico, fotos, etc.).

La regla general es que está prohibido copiar elementos confidenciales clasificados como **"Top Secret"**, sólo por razones excepcionales y previa aprobación de la persona responsable del *control confidencial.*

En este caso, la copia también debe ser registrada como se ha descrito anteriormente y esto también se considera como un nuevo documento con la versión original.

Los elementos **"Secret"** pueden ser divulgados solo a determinadas personas en la empresa, las que deben ser designadas y autorizadas por el responsable del *control confidencial.*

El control de la distribución debe ser realizado por un número de secuencia y es obligatorio.

Almacenamiento

Informaciones **"Top Secret"** y **"Secret"** deben ser almacenadas sólo en los lugares que pueden ser cerrados y con acceso restringido y controlado.

Está prohibido el almacenamiento de informaciones **Top Secret** en un ordenador personal o en un medio de almacenamiento externo.

Informaciones **Top Secret** solo pueden ser almacenadas en un servidor con la condición de que su acceso esté protegido por una contraseña.
Las contraseñas de seguridad deben tener su divulgación restringida sólo a las personas autorizadas y el responsable del Control Confidencial debe tener el respeto de estas personas.

Descartes

Una vez que la información confidencial se hace innecesaria, debe ser desechada a través de una autorización previa por parte del responsable de los controles confidenciales, este elemento de preferencia debe ser triturado, quemados, o cualquier otra acción que asegure que el mismo no pueda ser leído por cualquier persona no autorizada.

Las descargas de Información **Top Secret** deberá ser manejada por el Presidente o Gerente Senior de Operaciones de la organización.

Fotografías:

Como regla general está prohibido tomar fotografías en el interior de la empresa por motivos de seguridad y protección de la confidencialidad.

Los visitantes o proveedores que entren a la empresa no deben utilizar cámaras fotográficas, cámaras de video, teléfonos con cámara o cualquier otro dispositivo que fotografíe o filme.

Sin embargo como parte de nuestra operación implica la toma de fotografías controladas en algunos procesos de bodega e ingeniería, se permitirá la toma de estas bajo los siguientes parámetros:

- Cuando el colaborador necesite tomar fotografías con el fin de indicar las referencias de la empresa. En este caso el colaborador deberá utilizar una máquina o dispositivo fotográfico propiedad de la compañía y no deben usar dispositivos personales.

- En los procesos de empaque, despacho y recibo, como evidencia de que la mercancía:
    1. Se empaca de forma correcta,
    2. Se entrega en perfectas condiciones al contenedor o al agente transportista durante el proceso de la exportación.
    3. Se recibe con anomalías (cartones golpeados, rotos, faltantes, etc).

- Cuando el colaborador necesite tomar fotos con el objetivo de preparar una presentación para la empresa, también en este caso el colaborador deberá utilizar una máquina o dispositivo fotográfico propiedad de la compañía y no deben usar dispositivos personales.

- Se debe obtener previamente un acuerdo de confidencialidad, en caso de que un Gerente de Departamento autorice a una visita/proveedor para la toma de fotos en la compañía, de lugares predeterminados, siempre que el objetivo haya sido declarado de antemano y sea aceptable, siguiendo los lineamientos corporativos.

Colaboradores

Los trabajadores son los únicos permitidos en la Zona A y B, a través de la autenticación de su tarjeta de identificación, esto es implementado para controlar la entrada y la salida.

Proveedores de Servicios

El Departamento de Administración mantiene registros sobre la identificación de los proveedores y debe obtener un contrato con ellos incluyendo un acuerdo de confidencialidad cuando aplique.

Cuando una persona que no es colaborador tiene que entrar todos los días en un lugar clasificado como Zona A por razones comerciales, deben obtener autorización previa y estar acompañados del responsable de la zona visitada y circular con el pase de visitante a la vista.

Visitantes

El visitante tiene la obligación de registrarse en la entrada de la empresa, debe anotar sus datos (nombre, razón social, depto. donde se dirige, motivo de visita). Se debe completar el formulario requerido y firmar la Declaración de Confidencialidad, si es proveedor de servicios críticos.

Tomar fotos es en principio, prohibido.

El mismo debe circular con el pase de visitante a la vista.

Inspección

El equipaje o los bienes de uso personal en la bodega serán revisados a la entrada y a la salida, mediante dispositivos electrónicos y/o medios manuales.

Información y dispositivos de comunicación, medios de almacenamiento:

El almacenamiento de información confidencial en un medio extraíble debe ser previamente aprobado y registrado por la persona responsable del *control confidencial*: nombre del solicitante, indicar el objetivo, nombre del responsable de la aprobación, el nombre de la persona que transporta el medio dentro o fuera, y las fechas de las solicitudes deben ser registradas.

Cuando una negociación comercial, capacitación de personal o servicio post-venta requiera el uso de

dispositivos externos como medio de transporte de información; previamente se debe obtener la autorización de la persona responsable del *control confidencial* y *IT*, guardando registro del objetivo de la operación.

Educación y Entrenamiento:

Funcionarios permanentes y temporales: las *cláusulas de confidencialidad* deberán incluirse en los Contratos de Trabajo y en el Manual de Conducta Interno de KLA

Establecer un programa para difundir el conocimiento y la conciencia de los objetivos del control de la información confidencial para todos los funcionarios.

Los nuevos miembros de la empresa que inician su actividad en **KLA** deben ser informados, educados y estar conscientes de la obligación de cumplir con las disposiciones de la presente norma.

Los contratos con empresas tercerizadas para la prestación de servicios, ya sean temporales, proveedores o subcontratistas deben incluir una cláusula de confidencialidad sobre esta norma y del control de la información confidencial deben aceptar que existe un completo control de la seguridad de los elementos confidenciales de la empresa. Este punto podrá ser auditado por el responsable del *control confidencial*.

Todos los colaboradores externos al prestar servicios a la empresa deben registrarse en una hoja de control a la entrada que lleva el registro diario de las entradas y salidas de personas a la empresa.

Instrumentos para Controles, inclusive de Informaciones Electrónicas

1-Protección:

El responsable del área de Tecnología de Información - IT debe determinar los procedimientos preventivos para evitar el robo o la pérdida de computadoras, servidores y cualquier otro tipos de equipos de comunicación donde se haya almacenado información confidencial.

Las computadoras que son utilizadas diariamente por los funcionarios deben estar fijas en el escritorio por medio de cables y las que no se utilizan continuamente deben mantenerse en una habitación cerrada con llave, un armario o en una mesa en el caso de las notebooks.

*En caso de que el usuario por la naturaleza de su trabajo deba moverse entre oficinas o fuera de ellas, podrá hacer uso de una Laptop en lugar de un desktop.

Los dispositivos de almacenamiento de información deben ser almacenados de manera que no sea posible que personas no autorizadas puedan ver su contenido.

2-Control de Contraseñas:

La Identificación Personal (ID) y contraseñas de acceso de los funcionarios deben ser controlados para evitar que sean conocidos por personas no autorizadas.

Las contraseñas de acceso se cambian periódicamente.

3-Prevenciones contra Virus de computador y Fuga de Informaciones

Los equipos utilizados por los funcionarios, servidores de red y software antivirus designados por la empresa deben ser utilizados continuamente y actualizarse con regularidad para mantener la seguridad de la información.

Se debe orientar a los usuarios de computadoras para desconectar inmediatamente el cable de red entre el computador y el servidor de red en el caso de que un virus informático infecte la máquina que este usando el funcionario, e informar inmediatamente a la persona responsable de IT en la empresa.

En el caso de una infección por virus, el departamento de IT deberá identificar el tipo de virus, la forma en que se permitió la infección, la magnitud de los daños y tomar medidas preventivas inmediatas para limitar la propagación del virus y tomar las medidas necesarias para restablecer el sistema de seguridad y la eliminación del virus de la computadora del usuario.

Cuando un funcionario regresa de un viaje de negocios en el que se ha llevado su portátil de trabajo, deberá realizar un análisis completo de la unidad de disco duro una vez llegue a la empresa. Para ello hará uso del software designado por el departamento de sistemas. Esta medida deberá tomarse antes de conectar el equipo en la red informática de la compañía.

Precauciones

Establecer procedimientos para asegurar que la información confidencial en las computadoras o en los informes sobre los escritorios no sean vistos por personas no autorizadas.

Cuando por alguna razón el funcionario necesita alejarse de su lugar de trabajo, antes de hacerlo, debe bloquear la pantalla del computador con una contraseña.

El departamento de administración de IT, deberá hacer inspecciones con el fin de garantizar el uso adecuado de los equipos de comunicación e información y para comprobar la situación real del uso de estos equipos y si es necesario deberá determinar la aplicación de medidas correctivas dado el caso de mal uso.

Transporte de computadores y medios de almacenamiento en general

Está prohibido a los funcionarios llevarse el equipo fuera de la empresa, salvo en circunstancias excepcionales y cuando sea por motivos de trabajo y con autorización previa de la persona responsable del área de IT.

Los funcionarios pueden llevar sus computadoras portátiles en viajes de negocios, sin embargo deben obtener una autorización previa del responsable del área de IT.

Todos los departamentos deberán llevar un registro de las fechas en que los equipos tienen entradas y salidas de la empresa en conjunto con la declaración del objetivo de la operación.

Como ***regla general***, cuando sea necesario por razones de trabajo el uso de equipos o dispositivos de almacenamiento de información externos, el funcionario deberá obtener una autorización previa del responsable de IT.

Descarte, eliminación o cambio de Equipos de Informática y Comunicación

Cuando la empresa proceda al descarte/eliminación/cambio de un computador, servidor o cualquier otro dispositivo de almacenamiento de información, el responsable del Control de la Información Confidencial deberá asegurarse de que los datos han sido destruidos físicamente por lo que se puede garantizar que la información no será vista por personas no autorizadas.

Instalación y Configuración Segura del Sistema

En esta sección se seguirán los lineamientos establecidos en las Políticas de IT, obedeciendo todas las normas establecidas en la Política de Confidencialidad. A continuación se detallan los elementos que requieren un manejo seguro durante la instalación y configuración del sistema:

1. Preparación de la Instalación
2. Particionamiento
3. Documentación de Instalación y Configuración
4. Contraseñas de Administrador
5. Instalación Mínima de Software/Componentes relacionados con los servicios de red.
6. Desactivación de Servicios no utilizados
7. Instalación de Correcciones
8. Registros
9. DNS (Domain Name System)
10. Políticas de Backup y Recuperación del Sistema

11. Precauciones contra la Ingeniería Social

12. Firewall

13. Redes Wireless

Educación a los usuarios de equipos informáticos

El personal de IT constantemente debe promover la educación de los usuarios para evitar que por falta de conocimiento de las reglas, los conceptos y procedimientos básicos se vea afectada la seguridad del sistema.

Se deben establecer y distribuir las políticas de seguridad claras, sin ambigüedades, conocidas y comprendidas por los usuarios de la red.

Establecer un canal de comunicación donde a menudo información sobre temas relevantes de seguridad sean transmitidas a los usuarios de la red.

Controles internos

La persona designada para la promoción del control confidencial, deberá:

1. Obtener autorización del Top Management para hacer cambios en la política.
2. Revisar la política y la lista de ítems confidenciales identificados una vez al año.
3. Elaborar un Plan anual de promoción de la información confidencial (ejm.: bolletin board, anuncios de nuevos controles de seguridad de la información, otros).
4. Revisar el JTSG, asegurarse de monitorear los progresos de las mejoras al JTSG. Evidenciar reportes al Top Management de la implementación y progresos.

7.0 REGISTROS

Lista de Clasificación de la Información
Acuerdo de Confidencialidad
Compromiso de Confidencialidad

6.0 ANEXOS

– Anexo 1 – Estructura Organizacional del Comité para el Control de la Información Confidencial