POLITICA SEGURIDAD DE LA INFORMACIÓN

OBJETIVO:

Es política de Kimberly-Clark de México que el personal que por motivos de su trabajo tenga acceso, maneje o elabore información sensible o confidencial, se haga responsable de la custodia, uso, disposición o destrucción de la misma.

ALCANCE:

Esta Política aplica En Kimberly-Clark de México y Subsidiarias, en adelante KCM.

DEFINICIÓN:

Seguridad de la información se define como proteger, resguardar, cuidar y manejar la información elaborada o almacenada en cualquier medio, ya sea papel, sistemas, computadoras, discos duros de computadoras personales o de los llamados servidores ("servers"), discos flexibles, compactos (CD-ROM o DVD); así como planos, manuales, formulaciones, planes de negocios, de producción, expansión o contracción, etc., para prevenir que alguna persona ajena o no autorizada, tenga acceso a información de KCM que pudiera divulgar o utilizar y ocasionar algún perjuicio a la compañía.

PROTECCIÓN Y CLASIFICACIÓN DE LA INFORMACIÓN

La información debe clasificarse de la siguiente forma:

- **Public:** Información operativa de rutina, como informes públicos o descripciones generales de productos.
- **K-C Internal Use Only:** Categoría predeterminada, como listas de direcciones o reportes generales.
- **K-C Confidential:** Datos valiosos, como propiedad intelectual o listas de clientes.
- **K-C Sensitive:** Información sujeta a requisitos legales, como registros médicos o del seguro social.

Es responsabilidad de cada Gerente establecer y verificar los controles de protección para:

a) Identificar y clasificar la información que requiere manejo y cuidado especial.

b) Resguardar un duplicado de la información en un lugar seguro, para tenerla accesible en caso de un siniestro.

c) Asignar a una persona como responsable de la protección de la información identificada como sensible o confidencial.

d) Determinar quiénes deben tener acceso y quienes necesitan cada tipo de información y cómo debe manejarse la información clasificada.

e) Determinar quién y cómo debe moverse la información clasificada de un sitio a otro.

f) Instruir al personal para que todas las solicitudes externas de información clasificada que se reciban, sean referidas a la gerencia de su área para obtener aprobación expresa, antes de proporcionar cualquier dato.

g) Instruir a su personal para que eviten hablar con otras personas sobre la empresa o sus planes de trabajo, en lugares públicos tales como: elevadores, taxis, aviones, salas de espera, restaurantes, clubes, etc. Asimismo, cuidar los comentarios que se hagan sobre la empresa con familiares y amigos.

AUTORIZACIÓN

El Director y/o Gerente del área, son los únicos que pueden autorizar a los empleados, que por razones de su trabajo, deban tener acceso a la información clasificada como confidencial de su área o departamento.

MANEJO

Es responsabilidad del usuario de la información confidencial, que ésta no esté a la vista ni accesible, ya que otras personas ajenas a la empresa o a la función, puedan obtener datos sobre ella.

La información deberá tenerse en un lugar seguro y/o quitarla del monitor de la computadora cuando haya alguna persona cerca de su lugar o cuando el usuario se retire de su área de trabajo.

Siempre que se mueva información sensible, ya sea en papel, “USB” o cualquier medio electrónico, deberá colocarse en un sobre y entregarla en propia mano al destinatario.

ALMACENAMIENTO

El usuario de la información confidencial contenida en papel o medios electrónicos, tales como discos compactos, planos, manuales, planes de negocios, etc., debe asegurarse de guardarlos en un lugar con llave, cuando no esté en uso. Así mismo, asegurarse que quedan bajo llave cuando se retire de su oficina.

Los discos duros de la PC’s deben asegurar la integridad de la información, teniendo una clave de acceso (“password”) para protegerla.

Es responsabilidad de las gerencias tener un respaldo anticipado de la información contenida en las PC’s del personal que deja de prestar sus servicios en la empresa.

SISTEMAS ELECTRÓNICOS

Los usuarios de computadoras personales deben contar con clave de acceso para iniciarlas, así como para proteger la información confidencial. El correo electrónico (Outlook) puede utilizarse para enviar información confidencial a otras localidades de KCM, siempre y cuando se esté autorizado por el Gerente del área para realizar esta actividad; en estos casos, el archivo deberá enviarse protegido con clave de acceso proporcionada al destinatario por un medio distinto.

La clave de acceso de computadoras y redes de sistemas de comunicación nunca deben de proporcionarse a otra persona.

Las computadoras portátiles (laptops o notebooks), nunca deben dejarse al alcance de otras personas y deben guardase en un lugar seguro. Éstos equipo deben contar con clave de acceso para poderse iniciar y que nadie pueda usarlos.

DESTRUCCIÓN

La información confidencial en papel, cuando ya no sea útil debe destruirse utilizando un triturador de papel y en caso de los dispositivos electrónico deben inhabilitarse partiéndolos en varios fragmentos. En el caso de los discos duros de las PC’s deben ser formateados para eliminar la información que contengan. La información confidencial no debe ser depositada en las papeleras si no está triturada, destruida o inutilizada para que ninguna persona pueda hacer uso del contenido.