POLITICA SEGURIDAD DE LA INFORMACIÓN

Política	**Ejecutivo a cargo:**	**Persona de contacto:**
Dirección de Finanzas	Director de Finanzas	Subdirector de Servicios de Información Gerente de Infraestructura y Operaciones de T.I.

OBJETIVO:

Es Política de Kimberly-Clark de México que todo el personal se haga responsable de cuidar y salvaguardar la infraestructura tecnológica para proteger la información de la compañía y 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:

Aplica a 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, laptops, celulares, servidores, la Nube, para prevenir que alguna persona, no autorizada o ajena, tenga acceso a información de KCM y que pudiera divulgar o utilizar y ocasionar algún perjuicio a KCM.

RESPONSABILIDADES

1. El Director General pertenece al Consejo de Administración y se encarga de comunicar a los altos ejecutivos las decisiones tomadas en el Consejo de Administración que influyen en los temas económicos, sociales, ambientales, tecnológicos y de ciberseguridad. A su vez, los altos ejecutivos toman las decisiones pertinentes y lo comunican a los colaboradores.

2. La Subdirección de Servicios de Información es responsable de identificar los riesgos Tecnológicos y de Ciberseguridad, de existir alguno, se incluye en el portafolio de

riesgos, se evalúa y se implementan las medidas de mitigación, adicional KCM cuenta con la Política no. 60 “Administración de Crisis y el Plan de Continuidad del Negocio”.
El Departamento de TI será responsable de planear, ejecutar y dar seguimiento a los requerimientos dirigidos al personal KCM, así como el cumplimiento de los cursos en temas de
Seguridad de la Información / Ciberseguridad.

3. Es responsabilidad de cada Director / Subdirector / Contralor / Líder / Gerente establecer y verificar los controles de protección:
   a. Identificar y clasificar la información que requiere manejo y cuidado especial.
   b. Determinar quienes deben tener acceso, a que tipo de información y como deberá manejarse la información clasificada.
   c. Determinar quien y como debe moverse la información clasificada de un sitio a otro.
   d. Instruir al personal para que todas las solicitudes externas de información clasificada que se reciben, sean referidas al Director / Subdirector / Contralor / Líder / Gerente de su área para obtener aprobación expresa, antes de proporcionar cualquier dato.
   e. 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, entre otros. Asimismo, cuidar los comentarios que se hagan sobre la empresa con familiares y amigos.

4. Es responsabilidad de todo el personal de KCM reportar a su jefe inmediato superior el tema que pudiera poner en riesgo a KCM sobre Seguridad de la Información y Ciberseguridad y este a su vez lo reportará al Director / Subdirector / Contralor / Líder / Gerente y atenderá las indicaciones del Departamento de Servicios de Información.

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 (formulaciones o información propia de las marcas de productos, entre otros), listas de clientes, información de ventas, precios y descuentos a clientes, precios y volúmenes de materias primas y materiales.
- **K-C Sensitive:** Información sujeta a requisitos legales, como registros médicos o del seguro social.

AUTORIZACIÓN

El Director / Subdirector / Contralor / Líder / Gerente del área según aplique, 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 esta no esté a la vista ni accesible, ya que otras personas ajenas a la función o la empresa, pueden obtener datos sobre ella.

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

Siempre que se mueva información sensible en cualquier medio electrónico deberá de contar con la autorización Corporativa para hacerlo.

ALMACENAMIENTO

El usuario de la información confidencial contenida en papel, deberá de asegurarse de guardarlos en un lugar con llave, cuando no estén en uso. Así mismo, asegurarse de la correcta guarda y custodia cuando se retire de la oficina.

Es responsabilidad del Director / Subdirector / Contralor / Líder / Gerente solicitar un respaldo anticipado de la información contenida en las PCs / Laptops / Celulares asignados por la empresa solicitándolo al Departamento de Tecnologías de la Información del personal que dejará de prestar sus servicios en la empresa.

Importante: Se prohíbe el uso de ***computadoras, tabletas y teléfonos celulares personales***, para envío o almacenamiento de información de la empresa; se prohíbe almacenar y/o respaldar información de la empresa en dispositivos externos, como discos USB o memorias flash USB.

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 Director / Subdirector / Contralor / Líder / Gerente del área para realizar esta actividad.

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

Las PCs / Laptops / Celulares, nunca deben dejarse al alcance de otras personas y deben guardarse en un lugar seguro.

DESTRUCCIÓN / ELIMINACIÓN DE ARCHIVOS

Una vez pasado el periodo de retención de la información el Director / Subdirector / Contralor / Líder / Gerente o cualquier persona que maneje información confidencial deberá solicitar autorización de la Gerencia de Impuestos y de la Contraloría Corporativa para proceder con la destrucción o eliminación de archivos.

Cuando ya no sea útil la información confidencial en papel deberá de destruirse utilizando un triturador de papel y depositarla en las papeleras.

Los dispositivos electrónicos deben inhabilitarse partiéndolos en varios fragmentos. En el caso de los discos duros de las PCs / Laptops / Celulares, el Departamento de TI es el responsable de formatearlos para eliminar la información que contengan.

La información almacenada en la Nube en los ambientes de “OneDrive”, “Outlook”, “Share Point”, entre otros, deberá el Director / Subdirector / Contralor / Líder / Gerente, solicitar a TI los respaldos antes de que la persona deje de laborar en la empresa en coordinación con Recursos Humanos.