

---

# POLÍTICA DE CONFIDENCIALIDAD

---



Version	Version 1
History	June, 2017
Approval procedure	GMI/GS/Legal/Compliance/IT
Target Group	Danone employees & Suppliers / North LATAM cluster
Document Owner	Chief Compliance Officer
Level of Confidentiality	Internal Use
Number of Pages	7
Languages	Spanish

Danone S.A. is the exclusive holder of all copyrights related to this document. All rights reserved.

# ÍNDICE

---

<b>01. OBJETIVO Y CAMPO DE APLICACIÓN</b>	<b>4</b>
<b>02. DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL</b>	<b>4</b>
<b>03. CLASIFICACIÓN DE LA INFORMACIÓN</b>	<b>5</b>
<b>04. MEDIDAS DE SEGURIDAD</b>	<b>6</b>
<b>05. RECOMENDACIONES GENERALES</b>	<b>6</b>
<b>06. RIESGOS Y SANCIONES</b>	<b>7</b>

# 01 OBJETIVO

---

El objetivo de la presente política es proteger la información confidencial propiedad de Danone o de terceros que han confiado información a Danone con dicho carácter.

La presente política es de aplicación obligatoria para las empresas del Grupo Danone en el North LATAM Cluster (México, Centroamérica y Colombia).

Esta Política se complementa con la Política de Seguridad Informática.

# 02 DEFINICIÓN DE INFORMACIÓN CONFIDENCIAL

---

Información confidencial es toda información que represente una ventaja competitiva para la empresa, información que ha sido entregada a Danone con carácter confidencial o información sujeta a la protección de las leyes de datos personales.

La información confidencial puede ser generada por cualquiera de las empresas de Grupo Danone, sus proveedores o agencias. En todo caso, se trata de información que no debe de ser revelada sin el consentimiento o de acuerdo a los lineamientos establecidos en la presente política.

De manera enunciativa, a continuación se citan algunos ejemplos:

- Fórmulas de nuestros productos
- Planes estratégicos
- Planes de marketing
- Procesos industriales
- Lanzamientos de productos
- Conceptos o modelos de negocio
- Prototipos
- Diseños
- Información sobre nuevos negocios
- Bases de clientes
- Contratos con clientes, distribuidores, proveedores y socios
- Estudios de mercado

En caso de duda sobre la naturaleza de la confidencialidad de la información, los Danoners debemos asumir que se trata de información confidencial y tratarla como tal y consultar al área Legal.

## 03 CLASIFICACIÓN DE LA INFORMACIÓN

---

Para conocer cómo se debe manejar y cuidar adecuadamente la Información Confidencial, se debe tomar en consideración la siguiente clasificación:

- **Información Confidencial Ultra Sensible:** Información que sólo algunos miembros de la organización debería de conocer ya que existe un acceso restringido a la misma. (Ej. Información de un “Special Taskforce”)

Debe de existir un control específico de acceso y trazabilidad de las personas que tienen acceso a dicha información.

- **Información Confidencial Sensible:** Cualquier especie de información que en caso de ser conocida por algún tercero ajeno a la organización, ponga en riesgo la ventaja competitiva que Danone pudiera tener o comprometa los proyectos que se encuentra ejecutando o a punto de implementar. (Ej. Información relacionada con un “special pack” que está a punto de ser implementado).

Aquellas personas que tengan acceso a esta información, no deben compartirla o revelarla a menos que tengan autorización por escrito del departamento Legal.

- **Información Confidencial de Uso Interno:** Información que se refiera a eventos o actividades de la empresa cuyos destinatarios o usuarios son empleados y/o proveedores de servicios (Ej. “Danone Day”, “Campus for All”, Inducción Corporativa, capacitaciones WISE, entrenamientos comerciales, etc).

Dado que dicha información se refiere a eventos de Danone, debe evitarse que se comparta hacia el exterior a menos que se tenga aprobación del director de área.

- **Datos personales:** Cualquier información relacionada a una persona física y que por su naturaleza sensible o personal, no debe de ser compartida a menos que se cuente con la autorización expresa del interesado. (Ej. Edad, sexo, religión, preferencia sexual, etc).

Aquellas personas que tengan acceso a este tipo de información deberán consultar con el departamento Legal cómo manejar las bases de información y seguir lo establecido por la Política de Data Privacy.

## 04

## MEDIDAS DE SEGURIDAD

---

Para el caso de información Confidencial Ultra Sensible o Información Confidencial Sensible, es necesario cumplir con las siguientes medidas:

### Autores de la Información

Es obligación y responsabilidad del autor de la información tomar las siguientes medidas para proteger y salvaguardar la información:

- a) Marcar la información como “Confidencial Ultra Sensible” o “Confidencial Sensible”, según el caso.
- b) Proteger el acceso a esta información a través de claves o archivos de accesos restringido.
- c) Limitar el acceso a la información sólo a aquellas personas que requieran conocer del tema.
- d) En caso de tener conocimiento que la información ha sido compartida sin autorización, notificar al departamento Legal.

### Receptores de la Información

- a) No compartir la información a la cual tuvieron acceso.
- b) No copiar o duplicar la información a menos que sea estrictamente necesario.
- c) En caso de tener conocimiento que la información ha sido compartida sin autorización, notificar al departamento Legal.

## 05

## BUENAS PRÁCTICAS EN EL MANEJO DE LA INFORMACIÓN

---

- Evitar hablar de la información a la que se refiere esta política en público
- Respetar las políticas de IT y sólo usar redes seguras
- Sólo utilizar las herramientas que da la empresa para compartir información (**NO** correo personal, **NO** WeTransfer, **NO** Prezi, etc.)
- Asegurarse que el lugar en donde se deja la computadora, celular o documentos sea seguro.
- Guardar los documentos con información confidencial o sensible en carpetas con acceso restringido.
- Guardar bajo llave todos los documentos físicos que contengan información confidencial o sensible.
- Proteger tanto la información confidencial y la propiedad intelectual de la empresa como la de nuestros consumidores, clientes y socios comerciales.

- Incluir passwords en documentos con información sensible o confidencial.
- Dar un nombre clave a los proyectos.
- No compartir los passwords de mi computadora, correo o de cualquier otro dispositivo que pueda contener información confidencial o sensible.
- En caso de transmitir información a un tercero, es mandatorio que se firme un Convenio de Confidencialidad de manera previa.
- Delimitar el acceso a la información de acuerdo a la clasificación que se le dé a la misma.

# 06 RIESGOS Y SANCIONES

---

Las consecuencias de violar la confidencialidad de la información, hacer mal uso de ésta o compartirla sin la autorización correspondiente podrán ser:

1. La configuración de un delito sancionado por la legislación mexicana.
2. El posible pago de una indemnización al afectado.
3. La terminación de la relación laboral y/o contractual.

El incumplimiento de la Política de Confidencialidad no se tolerará en Grupo Danone y puede tener como resultado la aplicación de una sanción administrativa o laboral, de acuerdo con la severidad del incumplimiento.