

<b>Título</b> <b>PROGRAMA DE CONCIENCIACIÓN Y FORMACIÓN EN SEGURIDAD DE LA INFORMACIÓN</b>	<b>Número</b> 001
<b>Unidad de Origen</b> Seguridad de la Información y Continuidad de Negocio	<b>Fecha Emisión</b> 01.03.19
<b>Ámbito de Aplicación</b> PGA Solutions y Filiales de Brasil, Argentina, Perú, Colombia y México	<b>Entrada en vigor</b> 01.03.19
<b>Resumen</b> El siguiente documento representa el plan anual de Concienciación y Formación en Seguridad de la Información, estableciendo las directrices básicas para el tratamiento seguro de la información y la protección de los activos.	
<b>Responsable Actualización</b> Seguridad de la Información	<b>Fecha Actualización</b> 16.03.21
<b>Certificación del documento</b> Seguridad de la Información y Continuidad de Negocio	<b>Fecha Revisión</b> 16.03.21

## INTRODUCCIÓN

El Programa Anual de Concienciación y Formación en Seguridad de la Información, es el marco de referencia de seguridad aplicable a los activos y a la totalidad de los Sistemas que soportan la red de Información PGA Solutions y Filiales en todos los niveles, estableciendo las directrices básicas para el tratamiento seguro de la información y la protección de los activos. Dichas directrices deben seguir los principios tradicionales de seguridad, a la vez que los expande y adapta para cubrir los nuevos riesgos asociados.

**ÍNDICE**

- 1 Concienciación y Formación en Seguridad de la Información**
  - 1.1 Concienciación en Seguridad de la Información
  - 1.2 Formación en Seguridad de la Información
    - 1.2.1 Formación para Empleados, Personal Externo y Subcontratado
    - 1.2.2 Formación Certificada en Empresas Externas
- 2 Actividades**
- 3 Cronograma**

## 1.- Concienciación y Formación en Seguridad de la Información

Esta guía será conocida por todos los empleados de PGA como parte de su formación y concienciación en seguridad de la información.

### 1.1 Concienciación en Seguridad de la Información

Se establece las medidas de índole organizativa para minimizar los riesgos de pérdida, daño o acceso no autorizado a los datos, dispositivos de almacenamiento o documentos fuera de las horas de trabajo.

En ellos se especificarán las siguientes directrices:

- La documentación, informes y medios informáticos tales como cintas o discos, deberán guardarse bajo llave, especialmente fuera del horario de trabajo.
- La información sensible o crítica deberá ser guardada en un sitio seguro, bajo llave, cuando no se requiera, especialmente cuando la oficina esté desalojada.
- Las estaciones de trabajo, terminales e impresoras deben disponer de autenticación, llave u otro tipo de mecanismo en caso de permanecer desatendidos.
- Los buzones de correo no deben permanecer desatendidos si no están protegidos.
- En los entornos donde se maneje información confidencial cuyo soporte físico sea el papel, se deberán proteger las fotocopiadoras del uso no autorizado fuera del horario de trabajo.
- La información sensible o clasificada impresa debe recogerse inmediatamente de las impresoras.
- Se establecerán procedimientos de limpieza de escritorio y pantalla, de modo que los dispositivos de almacenamiento, documentación e información queden protegidos cuando el empleado abandone su puesto de trabajo.

### 1.2 Formación en Seguridad de la Información

Establece las medidas de índole organizativa con la finalidad de formar a los empleados, así como personal externo, subcontratado, entidades colaboradoras y clientes acerca del Cuerpo Normativo de PGA, así como de los procedimientos aplicables a cada usuario para el normal desempeño de sus funciones.

#### 1.2.1 Formación para Empleados, Personal Externo y Subcontratado

En el presente nivel se establecen las medidas organizativas, aplicables a empleados, así como personal externo y subcontratado.

- Se hará entrega a los usuarios de los siguientes documentos:
  - Documentación formativa, incluyendo:
    - ✓ La Política General de Seguridad de Información de la compañía, según se especifica en la norma de seguridad de la información de aplicación general.
    - ✓ La Normativa y los Procedimientos que cada usuario deba conocer y seguir para el normal desempeño de sus funciones.
- Serán de obligado cumplimiento para todos los usuarios de los sistemas, la siguiente formación de carácter general (siempre que se hayan implantado los controles especificados en cada caso concreto):
  - La Política de Seguridad de PGA.
  - Política de confidencialidad desarrollada en la normativa preventiva de fuga de información.

- Etiquetado de los activos y manejo de información (especificado en la clasificación y control de activos).
- Procedimientos de Incidentes de Seguridad.
- La Política de protección frente a software malicioso de la empresa.
- Política de uso del correo electrónico.
- Responsabilidades de los usuarios en la utilización de contraseñas.
- Las responsabilidades de los usuarios de los sistemas debido al uso de información de carácter personal.
- El personal de Desarrollo deberá conocer las normas relativas al desarrollo de software especificadas la 'Normativa para el desarrollo y mantención de sistemas'.
- Se impartirán seminarios de formación específica en aspectos de seguridad relacionados con cada una de las áreas de Sistemas de Información.
- La formación de los usuarios deberá garantizar que los procesos críticos para los sistemas son conocidos al menos por dos personas.
- A las entidades colaboradoras se les hará entrega de los manuales y procedimientos necesarios para el desempeño de sus funciones

### 1.2.2 Formación Certificada en Empresas Externas

A las medidas especificadas en el nivel anterior, se añadirán las siguientes:

- El personal especializado recibirá cursos de formación de seguridad certificados y reconocidos en empresas acreditadas, para el desempeño de sus funciones.

## 2.- Actividades

El programa de concienciación está formalizado, para que todo el personal tome conciencia de la importancia de la seguridad.

El programa de concienciación exige a los empleados realizar, al menos, una vez al año, una declaración escrita o electrónica de que leyeron y entendieron la política de seguridad de la información de la empresa.

El programa formaliza la realización de capacitaciones al personal inmediatamente después de contratarlo y, al menos, una vez al año.

Se informa y educa a los empleados en lo que respecta a la concienciación por diversos métodos comunicacionales, por ejemplo:

- Carteles.
- Correos electrónicos corporativos.
- Capacitaciones presenciales o en línea.
- Reuniones.
- Promociones.
- Boletines, entre otros.

**3.- Cronograma**

Capacitaciones al personal inmediatamente después de contratarlo y, al menos, una vez al año en el primer semestre del año.

Se informa y educa a los empleados en lo que respecta a la concienciación, una vez cada tres meses, al menos mediante un Correo electrónicos corporativos, respecto a las políticas y normas de seguridad.