



**YOPDev**

POLÍTICA MARCO DE  
CIBERSEGURIDAD

## Contenido

Objetivo	2
Generalidades	2
Principios básicos	2
Modelo de Gestión	2
Política	3

---

## 1. Objetivo

---

Definir la política marco de ciberseguridad.

## 2. Generalidades

---

**YOPDev** considera que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar la correcta operación de los servicios de la organización y el cumplimiento de las obligaciones legales y contractuales.

La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la empresa, así como los activos que participan en sus procesos.

Esta Política tiene como objeto establecer el marco bajo el cual la organización garantiza la confidencialidad, integridad y disponibilidad de la información propia y de sus clientes, así como el cumplimiento de las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre la los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Esta política Marco de Ciberseguridad es de aplicación a todos los directivos, empleados, y proveedores de YOPDev.

## 3. Principios básicos

---

Para ello se establecen los siguientes principios básicos:

- Garantiza que los Sistemas de Información que dispone para la operación y prestación de sus servicios poseen el adecuado nivel de seguridad.
- Sensibiliza a todos los empleados, contratistas y colaboradores acerca de los riesgos de ciberseguridad y garantiza que disponen de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de la organización.
- Potencia las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las nuevas amenazas.
- Se dota de métodos y herramientas que permiten adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas.

## 4. Modelo de Gestión

---

**YOPDev** promueve un modelo de gestión aplicable a la Ciberseguridad basado en la normativa internacional ISO/IEC 27001, de modo que facilita, por todos los medios a su alcance y de forma proporcional a las amenazas detectadas, los recursos

---

necesarios para que la organización disponga de un entorno alineado con los objetivos de negocio y los objetivos de ciberseguridad establecidos.

El modelo definido por **YOPDev** se basa en:

- Un marco para la gestión de las medidas de ciberseguridad aplicables mediante un método de evaluación de riesgos, alineado con la estrategia y los objetivos de negocio y coherente con el contexto donde se desarrollan las actividades de la organización.
- Mecanismos para alinear los objetivos con la conformidad de los requisitos legislativos, reguladores y contractuales.
- Mecanismos para reaccionar frente a los incidentes que se produzcan tanto en la gestión del sistema como en los procedimientos operativos que dependen del mismo.
- La existencia de un conjunto de funciones y responsabilidades en materia de ciberseguridad claramente definidas.
- Un proceso de revisión, actualización y mejora continua de la presente política y del modelo de gestión de la ciberseguridad.

## **5. Política**

---

### **5.1 De la Información Interna**

- La información es un activo vital y todos sus accesos, usos y procesamiento, son consistentes con la criticidad, en cumplimiento con la confidencialidad y propiedad intelectual de la misma.
  - La información es protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas, sus procesos asociados y requisitos legales y contractuales.
  - La Alta Dirección provee los recursos que permiten implementar los controles necesarios para otorgar el nivel de protección correspondiente al valor de los activos.
  - Toda la información creada o procesada por la organización es considerada como “Confidencial”, a menos que se determine otro nivel de clasificación.
  - Periódicamente se revisa la clasificación, con el propósito de mantenerla o modificarla según se estime apropiado.
  - La organización provee los mecanismos para que la información sea accedida y utilizada por el personal, terceros y/o clientes que de acuerdo a sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar dicho privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.
-

## **5.2 De la Información de los Clientes**

- La información suministrada por el cliente o la procesada en nombre de este, será siempre considerada de su propiedad y recibirá el carácter de confidencialidad establecido por el mismo.
- Si la organización procesa y mantiene información de clientes que sean datos personales y/o sensibles de acuerdo a la normativa vigente, la organización se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna, y en cumplimiento con los lineamientos legales y contractuales.
- Si se requiere compartir información de los clientes con otras organizaciones, con motivo de externalizar servicios, a éstas se le exigirá la firma de un contrato de confidencialidad y no divulgación, previo a la entrega de la información.

## **5.3 Responsabilidades del Personal**

- La información y las tecnologías de información son usadas sólo para propósitos relacionados con el servicio y autorizados por los supervisores, aplicando criterios de buen uso en su utilización.
- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
- El personal tiene la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos establecidos en el manejo de incidentes.
- Está absolutamente prohibido al personal de la organización divulgar cualquier información de clientes así como toda aquella que esté catalogada como “Confidencial y/o Secreta”.
- Todo el personal a su ingreso firma un acuerdo de confidencialidad, el cual otorga todo el marco legal de protección contra la divulgación y propiedad intelectual de la información a la que acceda, procese y/o genere durante la vigencia de su contrato laboral y después de finalizado el mismo.

## **5.4 Compromiso de la Alta Dirección**

- La Alta Dirección vela por el cumplimiento de la presente política y suministra los recursos necesarios para el cumplimiento de la misma.
  - La Alta Dirección propicia la existencia de mecanismos y/o procedimientos formales que permiten asegurar la continuidad del negocio ante situaciones que impidan el acceso a la información imprescindible para el funcionamiento de la organización y los servicios prestados a clientes.
-

- La Alta Dirección procura que todo el personal reciba un entrenamiento suficiente en materia de seguridad, consistente con sus necesidades y su rol.
  - La Alta Dirección dispone la presente política a todo el personal, cliente y parte interesada.
-