
# SISTEMA DE GESTIÓN DE LA CALIDAD NTC - ISO 9001:2015

Entelgy

# MISIÓN

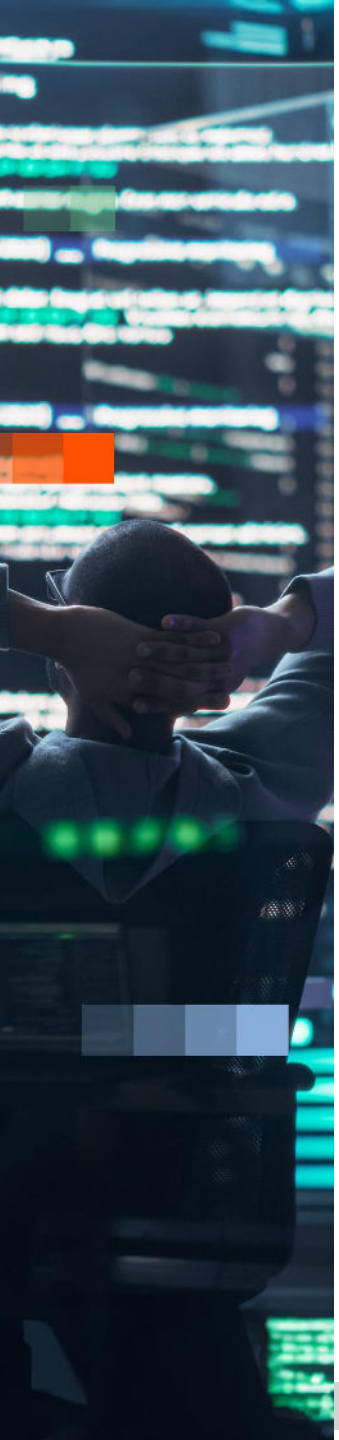
Generar una gran satisfacción a nuestros clientes y profesionales que son nuestra razón de ser.

# VISIÓN

Ser una empresa que se caracterice por la constante innovación, ser referente en el mercado por tener los más altos estándares en Bienestar a los empleados y lograr un desarrollo sostenible y rentable de cara al 2030.

# ALCANCE DEL SISTEMA DE GESTIÓN DE CALIDAD ISO 9001:2015

Desarrollo de software, servicios de Ciberseguridad y Servicios Técnicos Profesionales en Tecnologías de Información.



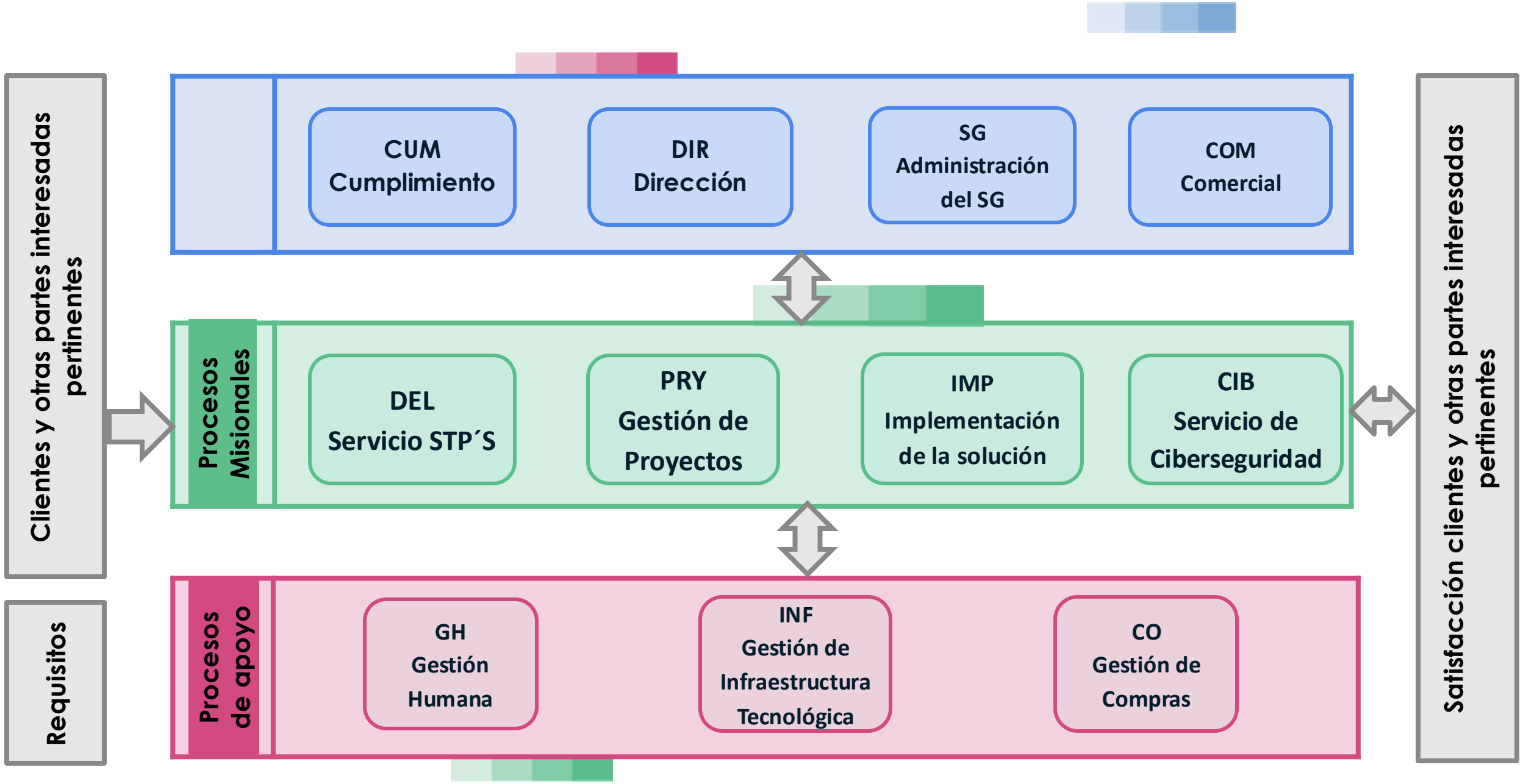
# POLÍTICA DEL SISTEMA DE GESTIÓN DE CALIDAD

**ENTELGY COLOMBIA S.A.S., busca satisfacer las necesidades y expectativas de sus clientes** en el Desarrollo de Software, Servicios de Ciberseguridad y Servicios Técnicos Profesionales en Tecnologías de Información, garantizando **el cumplimiento de los requisitos legales y reglamentarios** aplicables y promoviendo **la mejora continua del Sistema de Gestión de Calidad.**

Buscamos la fidelización y generación de crecimiento tanto en nuestros clientes actuales como en los nuevos, para lo que **enfocamos nuestros esfuerzos en la gestión comercial.** Así mismo, nos comprometemos a desarrollar nuestros servicios con **el aseguramiento en el cumplimento de los márgenes de la organización**, para lo cual **contamos con personal competente** que nos permite garantizar un adecuado desempeño en las labores encomendadas.

# OBJETIVOS DEL SISTEMA DE GESTIÓN DE CALIDAD

- Garantizar la conveniencia, adecuación, eficacia y mejora continua del Sistema de Gestión de Calidad.
- Dar cierre a las acciones correctivas que se establezcan para la mejora del SGC.
- Garantizar el cumplimiento de los requisitos legales y otros requisitos.
- Garantizar la satisfacción de nuestros clientes con base en sus necesidades y expectativas.
- Garantizar la respuesta oportuna y eficaz de las solicitudes, quejas y reclamos de los clientes.
- Establecer estrategias comerciales con el propósito de incrementar las ventas de la organización.
- Mejorar la competencia del personal a través del programa de capacitación continua.
- Implementar los requerimientos humanos, de manera adecuada y oportuna garantizando el cumplimiento de la oferta de servicio.


Clientes y otras partes interesadas pertinentes
Requisitos
CUM
Cumplimiento
DIR
Dirección
SG
Administración del SG
COM
Comercial
Procesos Misionales
DEL
Servicio STP´S
PRY
Gestión de Proyectos
IMP
Implementación de la solución
CIB
Servicio de Ciberseguridad
Procesos de apoyo
GH
Gestión Humana
INF
Gestión de Infraestructura Tecnológica
CO
Gestión de Compras
Satisfacción clientes y otras partes interesadas pertinentes

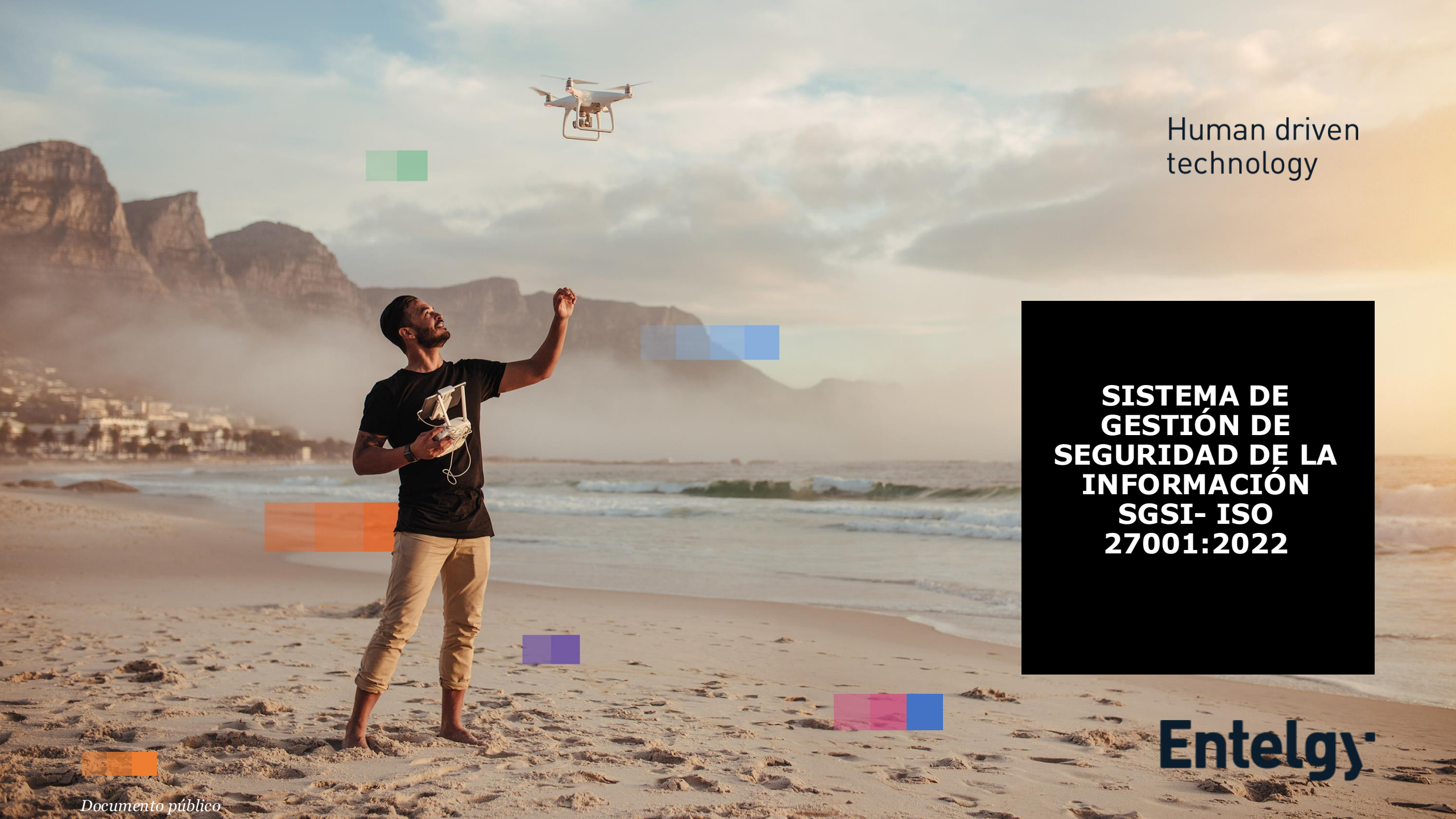
# PARTES INTERESADAS

El concepto de partes interesadas se extiende más allá del enfoque únicamente al cliente. Es importante considerar a todas las partes interesadas pertinentes. NORMA TÉCNICA COLOMBIANA NTC-ISO 9000 (Segunda actualización).

Parte del proceso para la comprensión del contexto de la organización es identificar sus partes interesadas. Las partes interesadas pertinentes son aquellas que generan riesgo significativo para la sostenibilidad de la organización si sus necesidades y expectativas no se cumplen. Las organizaciones definen qué resultados son necesarios para proporcionar a aquellas partes interesadas pertinentes para reducir dicho riesgo. Las organizaciones atraen, consiguen y conservan el apoyo de las partes interesadas pertinentes de las que dependen para su éxito.

# PARTES INTERESADAS

- Organización
- Accionistas
- Aliados
- Clientes
- Empleados
- Proveedores
- Comunidad
- Entes de Control



Human driven technology

# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI- ISO 27001:2022

Entelgy

*Documento público*


**Entelgy Colombia** cuenta con un **sistema de gestión de seguridad de la información** basado en la norma **ISO27001:2022**, que nos permite mejorar la postura de seguridad de los activos de información.

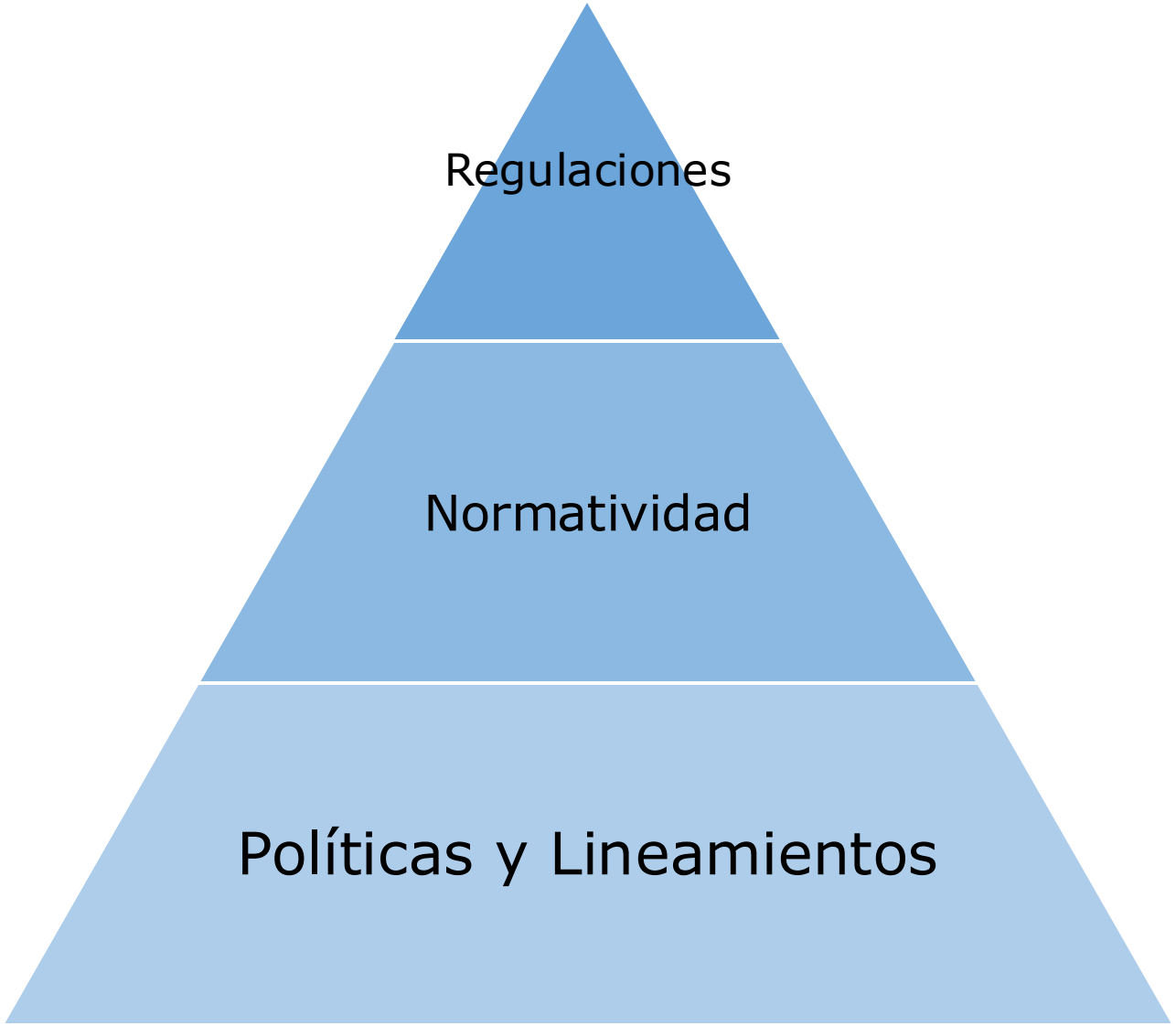
# Pilares de la Seguridad


**Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada

**Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Integridad**: Propiedad de la información relativa a su exactitud y completitud

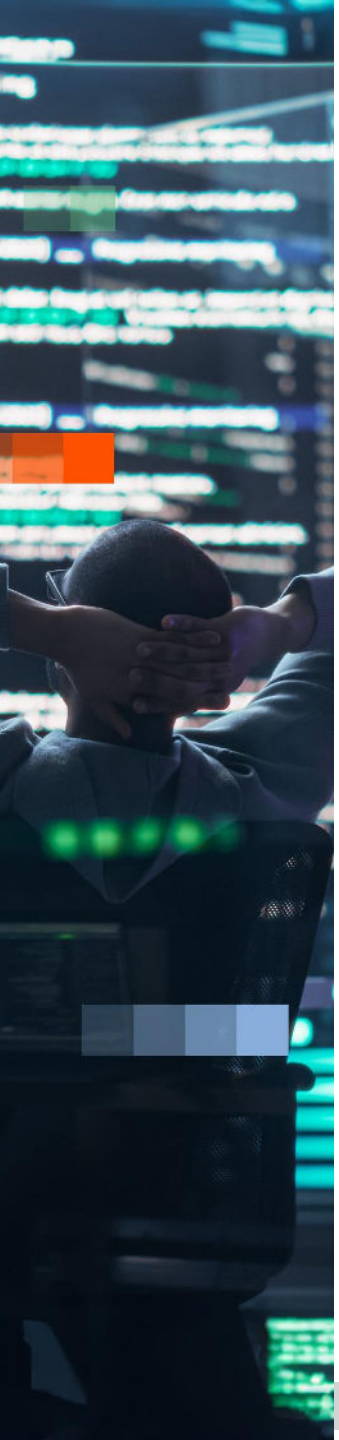
# Normatividad




- **Ley 1581:** 2012 Protección de datos Personales
- **Ley 1273:** 2009 De la Protección de la Información y de los datos

- **ISO 27001:2022**
- **ISO27002:2022**

- POL-ENT-DIR-01 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
- MAN-ENT-DIR-02 MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓ
- POL-ENT-CO-01 POLÍTICA DE GESTIÓN DE PROVEEDORES



# Política de Alto Nivel

Entelgy Colombia, dentro de su estrategia global para el desarrollo del negocio y el cumplimiento de sus objetivos, busca satisfacer las necesidades de las partes interesadas a través de la protección de los activos de información.
Estamos comprometidos en afianzar al máximo los servicios que prestamos a nuestros clientes, garantizando y promoviendo una cultura de seguridad de la información enmarcada en los principios de integridad, confidencialidad y disponibilidad de los datos, sistemas y/o conexiones de Entelgy Colombia.
Lo anterior, se logrará estableciendo y mejorando continuamente el sistema de gestión de seguridad de la información bajo estándares internacionales, así como; dando cumplimiento a las políticas, objetivos y otros requisitos aplicables que en ella se definan y/o apliquen.

**POL-ENT-DIR-01 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

# Roles y responsabilidades

| ROL | RESPONSABILIDAD |
|---|---|
| **Director General** | Aprobar la Política de Seguridad de la Información. |
| | Liderar y fomentar a todos los niveles la seguridad de acuerdo con la Política de Seguridad y los objetivos que en ella se definen. |
| | Asignar las responsabilidades y recursos para la gestión de la seguridad de la información. |
| | Tomar decisiones frente a los resultados de evaluación de riesgos de seguridad y privacidad de la información, que impacten negativamente la estrategia u objetivos del negocio. |
| | Desarrollar las revisiones del SGSI |
| **LISO** Local Information Security Officer | Establecer y mantener las estrategias de seguridad de la información y continuidad de negocio alineada con los objetivos de la organización, requerimientos regulatorios y contractuales. |
| | Ejercer el seguimiento y control de los SGSI y SGCN, coordinando la implementación de acciones de mejora y ajustes necesarios para el logro de los objetivos, informando a la alta dirección sobre el desempeño de los mismos. |
| | Promover al interior de la compañía la identificación, gestión y control de los riesgos de seguridad de la información enmarcados en el alcance de los sistemas, aplicando la metodología de gestión de riesgo. |
| | Promover y participar en la aplicación de auditorías internas y de tercera parte enfocadas a la seguridad de la información y continuidad de negocio. |
| | Definir las Políticas y procedimientos de seguridad de la información y continuidad de negocio alineados al cumplimiento y necesidades de la organización |
| | Fortalecer los planes de entrenamiento y sensibilización para los colaboradores en lo referente a seguridad de la información y continuidad de negocio. |
| | Coordinar y participar activamente en el grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad y/o ciberseguridad dentro de la organización y con posible afectación en cliente. |
| | Definir y gestionar los recursos necesarios para desempeño y eficacia de los sistemas de gestión SGSI-SGCN. |
| | Participar en los Comité Corporativo Seguridad |
| | Cumplir con los procedimientos documentados y estándares establecidos dentro de los sistemas de gestión. |
| | Apoyo y ejecución en el ciclo de los servicios contemplados en el proceso de ciberseguridad para clientes y/o área interna de la organización |

# Roles y responsabilidades

| ROL | RESPONSABILIDAD |
|---|---|
| **Infraestructura Tecnológica** | Apoyar y permitir que las políticas de seguridad de la información sean implementadas y mantenidas. |
| | Mantener toda la infraestructura de TI inventariada y monitoreada, con el fin de garantizar que cualquier robo o pérdida es detectado. |
| | Establecer los planes de recuperación de desastres. |
| **Infraestructura Tecnológica - primera línea de defensa** | Atender los incidentes de seguridad informática y supervisar las acciones realizadas en caso de que sean gestionadas por un proveedor de seguridad. |
| | Participar en el desarrollo de procesos y controles para la gestión de riesgos |
| **Compras** | Incluir las cláusulas de seguridad de la información en los contratos con proveedores o terceras partes a cargo o su alcance. |
| | Dar los lineamientos para la supervisión de los contratos a cargo o su alcance. |
| | Coordinar y/o supervisar la seguridad y los accesos físicos a las instalaciones de la organización. |
| | Gestionar el buen uso de los recursos económicos y financieros. |
| **Gestión Humana** | Incluir las cláusulas de seguridad de la información en los contratos con terceras partes a cargo o su alcance. |
| | Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. |
| | Cumplir con las leyes, normas y procedimientos establecidos para la selección, contratación, permanencia y finalización de la relación contractual de los Profesionales o Colaboradores de Entelgy Colombia. |
| | Informar el ejercicio de los derechos de los titulares de los datos personales a los Profesionales o Colaboradores. |
| **Responsable de Calidad** | Controlar la información documentada frente a los estándares de calidad. |

# Roles y responsabilidades

| ROL | RESPONSABILIDAD |
|---|---|
| **Responsable Jurídico/Legal** | Asesorar a la organización frente a los requisitos legales, reglamentarios y contractuales para la seguridad de la información. |
| **Oficial de Cumplimiento** | Definición de lineamientos en materia de protección de datos personales. |
| | Asesorar a la organización frente a los requisitos legales para la protección de los datos personales. |
| | Tramitar las consultas, solicitudes y reclamos de protección de datos. |
| **Profesionales o Colaboradores** | Cumplir con las políticas, lineamientos, procesos, procedimientos y asistir a las sensibilizaciones y capacitaciones del Sistema de Gestión de seguridad de la información SGSI |
| | Informar oportunamente cualquier evento o incidente de seguridad de la información |
| | Identificar los activos de información |
| | Participar en los análisis de riesgos y en la mitigación de los mismos acordes a sus funciones y/o cuando se requiera |
| **Proveedores y/o terceras partes** | Acatar las políticas de seguridad establecidas para los servicios prestados a Entelgy |
| **Auditoría Interna** | Elaborar el plan, programa |
| | Evaluar el cumplimiento de los requisitos de seguridad y/o aquellos definidos en los alcances de la auditoría interna. |
| | Elaboración del informe |

# Políticas de Seguridad

Cumplir con las políticas y procedimientos establecidas en este documento y el manual de políticas de seguridad

Cumplir con las leyes y normativas en materia de seguridad y privacidad de datos personales

Quien acceda a información de propiedad o tratada por Entelgy y en particular la de sus clientes, será consciente de sus responsabilidades en el mantenimiento de un nivel apropiado de seguridad de la información

Cada colaborador es personalmente responsable de garantizar que no se produce ninguna violación de la seguridad de la información como resultado de sus acciones

Los Profesionales o Colaboradores que trabajan desde ubicaciones externas deben cumplir con las directivas respecto a la seguridad en el acceso remoto.

Los Profesionales o Colaboradores deben informar al responsable de Seguridad de cualquier sospecha de incumplimiento o riesgo en materia de seguridad, tanto por acciones propias como por acciones de terceros.

Los Profesionales o Colaboradores deberán participar activamente en los programas de formación y conciencia en seguridad

El incumplimiento de estas normas puede derivar en acciones disciplinarias y/o procedimientos legales emprendidos contra el infractor. Los contratos con proveedores también requerirán que los contratistas y otras terceras partes cumplan con las disposiciones de la presente Directiva

## Decálogo de Seguridad

Los Profesionales o Colaboradores deben cumplir las políticas de continuidad de negocio, así como participar activamente en los planes de recuperación de acuerdo con su rol.

Los Profesionales o Colaboradores deben acceder apropiadamente a la información acorde a los privilegios otorgados por la organización

# POLÍTICA DE GESTIÓN DE PROVEEDORES

**Los proveedores de servicios que utilicen sistemas de información, o que procesen y almacenen datos de Entelgy Colombia, deberán cumplir con los estándares establecidos en la Política de Seguridad de la Información y el marco normativo correspondiente. Esto incluye, entre otros aspectos:**

- El incumplimiento de estas normas puede resultar en acciones disciplinarias o procedimientos legales contra el infractor. Además, los contratos y órdenes de compra con proveedores exigirán que los contratistas y otras terceras partes cumplan con las disposiciones de esta Directiva.
- Los proveedores que brinden sus servicios a la entidad preferiblemente tengan certificaciones vigentes relativas a la seguridad de la información, aplicada a los procesos de servicios que se contraten.
- Todos los contratos o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información, se realicen acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información.
- En las situaciones en que se requiera contratar servicios de tratamiento o protección de activos de información, tales como servicios de hosting e infraestructura, plataforma tecnológica, centros de datos y procesamiento, almacenamiento de información física y/o digital, entre otros, se deberá verificar que el proveedor cuenta con los mecanismos y controles de seguridad adecuados al objeto del servicio contratado
- Se deberá realizar una evaluación de requisitos de seguridad asociados al servicio entregado por el proveedor, con la finalidad de identificar brechas que puedan ser potenciales vulnerabilidades que expongan la continuidad operativa de las áreas y/o procesos o que puedan dañar la imagen corporativa.
- Establecer un procedimiento para la gestión de incidentes de seguridad y reportar cualquier incidente al supervisor del servicio y/o área administrativa.

Human driven technology

# MODELO CMMI ENTELGY COLOMBIA

Entelgy

*Documento público*

# ¿QUÉ ES EL MODELO CMMI?

El Modelo Integrado de Madurez y Capacidad (CMMI) es un conjunto probado de mejores prácticas globales que conducen el desempeño del negocio mediante la construcción y evaluación de capacidades clave.

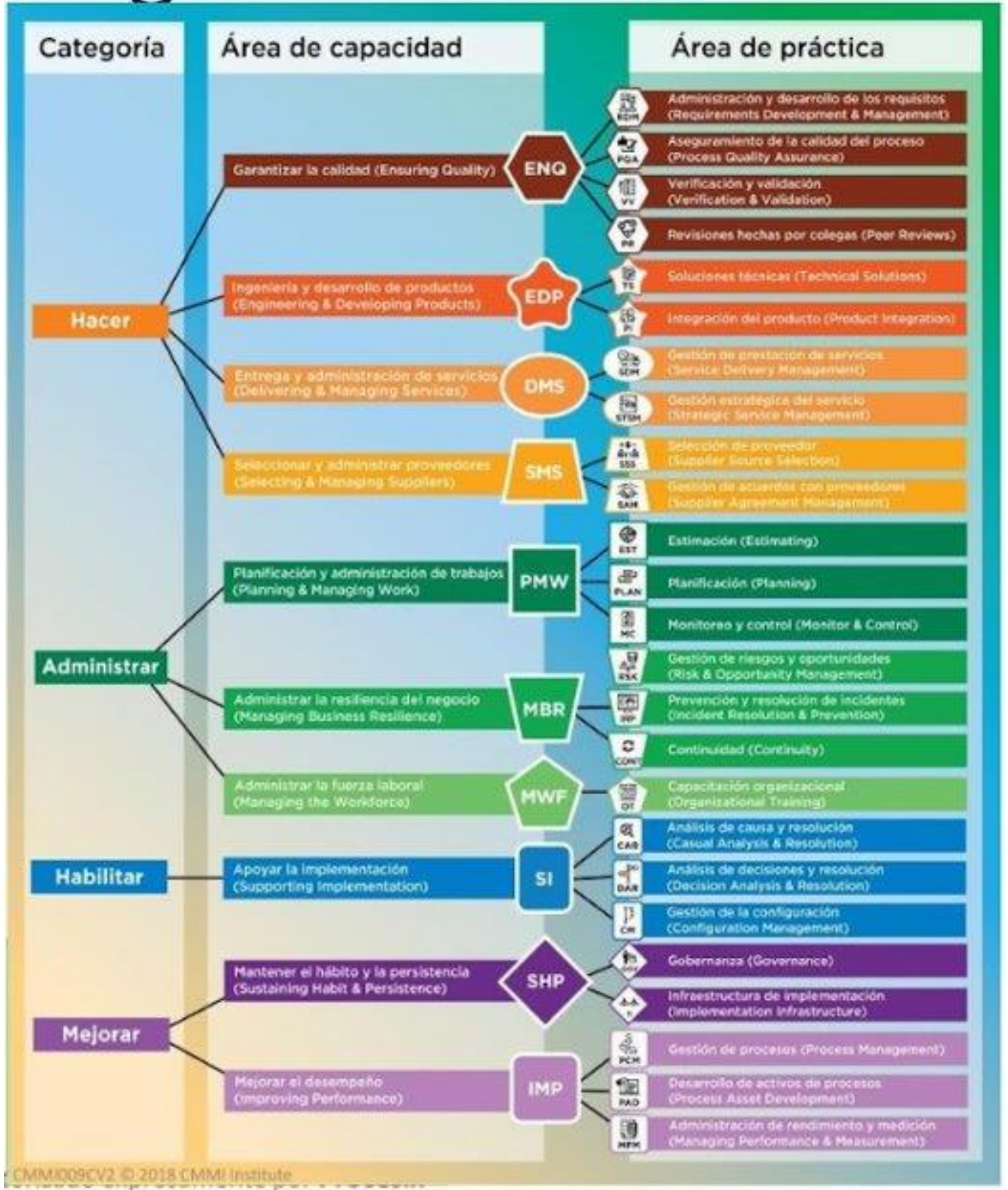
Las mejores prácticas de CMMI se centran en lo que se necesita hacer para mejorar el rendimiento y alinear las operaciones con los objetivos empresariales.

CMMI no es una metodología. CMMI nos dice qué buenas prácticas implementar, pero no nos dice exactamente cómo. Es un "framework", un conjunto de buenas prácticas organizadas por capacidades críticas de negocio con el objetivo de mejorar su rendimiento.

El modelo CMMI está dividido en: Categorías, áreas de capacidad y áreas de práctica

Una **Categoría** agrupa capacidades que cubren problemas comunes que afectan a los negocios

Las **áreas de capacidad** representan las capacidades de una organización para realizar y mejorar su procesos, estas evalúan la capacidad de la organización para llevar a cabo prácticas específicas




Entelgy
Human driven technology

Las **áreas de práctica** describen un modelo coherente de prácticas relacionadas entre sí. Estas prácticas representan actividades claves que una organización debe realizar para lograr mejoras en un área específica.

Una **Práctica** es el elemento más detallado del modelo, siendo una actividad que aporta valor y tiene un propósito

# Ciclo de Vida de Proyectos

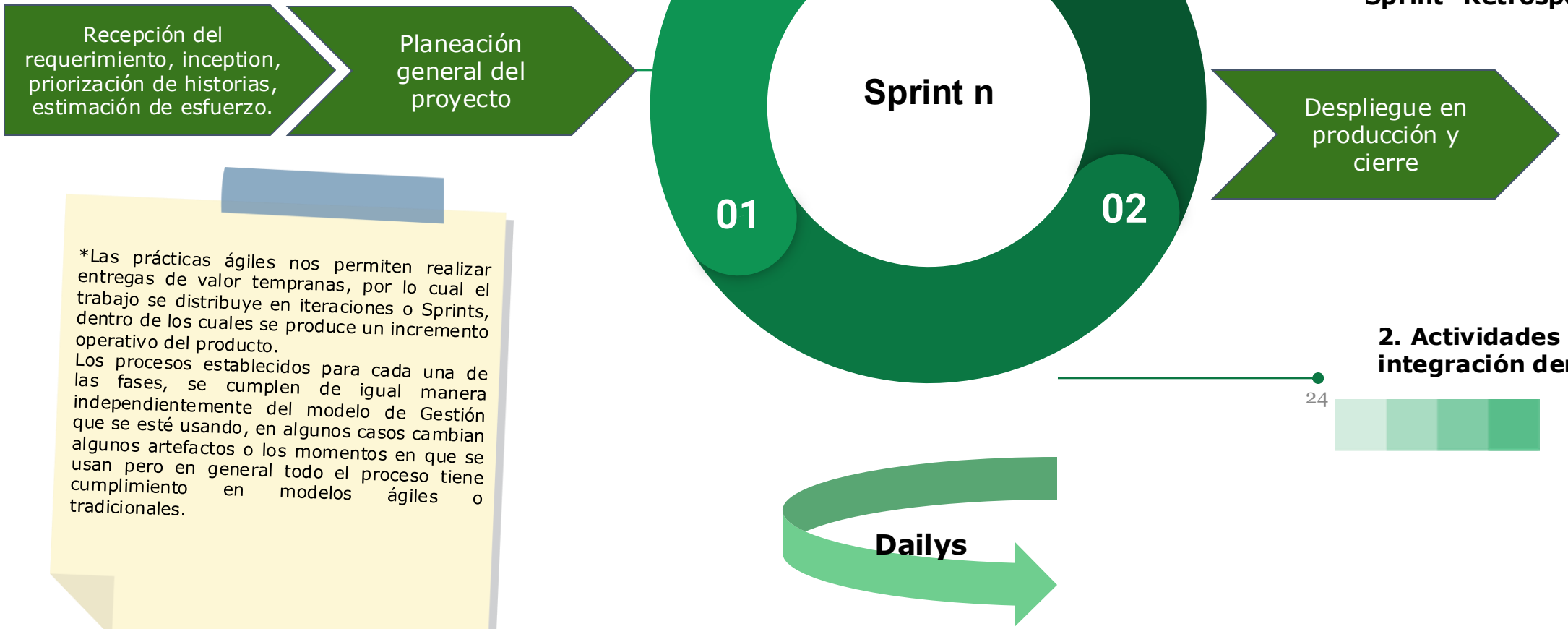
Entelgy
Human driven technology

| Gestión de Requerimientos | Planeación | Desarrollo e Integración | Control de Calidad | Producción y Cierre |
|---|---|---|---|---|
| Esta etapa comprende desde la recepción del requerimiento o necesidad del cliente, hasta la estimación y diseño funcional o propuesta comercial entregados al cliente para su aprobación | Una vez el cliente ha aprobado la ejecución del proyecto inicia esta fase en donde se planea a detalle todo lo requerido para la adecuada ejecución del proyecto: tareas, recursos, plazos, etc. | En esta etapa se realiza la construcción del producto de acuerdo al plan. | En esta etapa se realizan pruebas que garanticen que el producto entregado cumple con las especificaciones realizadas por el cliente en su requerimiento.<br>También se brinda soporte sobre las pruebas realizadas por el cliente | En esta etapa se realiza el paso a producción del producto y el cierre del proyecto |



**Monitoreo y Control**

# Uso del modelo con prácticas ágiles...




*Las prácticas ágiles nos permiten realizar entregas de valor tempranas, por lo cual el trabajo se distribuye en iteraciones o Sprints, dentro de los cuales se produce un incremento operativo del producto.
Los procesos establecidos para cada una de las fases, se cumplen de igual manera independientemente del modelo de Gestión que se esté usando, en algunos casos cambian algunos artefactos o los momentos en que se usan pero en general todo el proceso tiene cumplimiento en modelos ágiles o tradicionales.


24

# Entelgy

Human driven
technology