

# Lineamientos

## de las Tecnologías de la Información y las Comunicaciones (TIC)

<b>Versión:</b>	1
<b>Fecha de aprobación:</b>	27/04/2023
<b>Proceso responsable:</b>	Tecnología
<b>Aprobado por:</b>	Hugo Fernando Canaval Murillo

## Lineamientos Política de las Tecnologías de la Información y las Comunicaciones (TIC)

### 1. Objeto

Definir los detalles de cómo se debe implementar la Política de Tecnología de la Información y las Comunicaciones – TIC de Celsia, que se consiguen con la aplicación de estos lineamientos para gestionar las TIC.

### 2. Alcance

Estos lineamientos son aplicables a todos los colaboradores de Celsia, empresas vinculadas, consultores, aliados y terceras partes, que usen las TIC de la organización.

Los lineamientos deben ser revisados como mínimo una vez al año o cuando sea necesario.

### 3. Descripción de los lineamientos:

#### 3.1 Gobierno de las TIC:

- *La actualización del software y las librerías solo pueden ser gestionadas por los Product Manager (PM), considerando que, para el software de proveedores, las actualizaciones y migración a nuevas versiones se deben realizar antes de que termine la vigencia del soporte; ciñéndose a lo definido en el procedimiento de gestión de cambios.*
- *Garantizar la disponibilidad, integridad, confidencialidad, confiabilidad y continuidad de los productos y servicios tecnológicos bajo su gobierno, así como de la gestión del código fuente de las aplicaciones.*

#### 3.2 Adquisición e implementación de soluciones Tecnológicas

- *Establecer una segregación de ambientes, (Desarrollo/Calidad y Producción), considerando:*
  - *Definir y documentar las reglas para el paso de software entre ambientes.*
  - *El uso de diferentes equipos, directorios y dominios para las TO, cuando así aplique.*
  - *La restricción de uso de compiladores, editores y otras herramientas de desarrollo o recursos del sistema en ambientes de producción.*
  - *Los ambientes de pruebas deben emular el ambiente productivo tan real como sea posible.*
  - *Los menús de las aplicaciones deben mostrar mensajes de identificación adecuados para reducir el riesgo de error.*
  - *La restricción de uso de datos de producción en ambientes de prueba. En caso de ser necesario se debe utilizar un mecanismo de enmascaramiento siempre que sea posible.*

#### 3.3 Respaldo de la Información

- *Para los sistemas que se encuentran en nube no aplica backup en medios magnéticos y en su lugar se usan almacenamientos tipo archive.*
- *Todos los medios magnéticos deben ser etiquetados, de acuerdo con la clasificación y manejo de la información establecida por la organización.*
- *Se deben realizar pruebas de restauración de los backup anualmente para garantizar su correcto funcionamiento y calidad. Estas pruebas se planean de acuerdo con el documento BIA (Business Impact Analysis) donde están plasmadas las aplicaciones críticas de negocio.*

#### 3.4 Gestión de equipos e infraestructura

- *La asignación de extensiones telefónicas y modificación de categorías de acceso telefónico a la red pública conmutada se hará de acuerdo con las necesidades del servicio.*
- *Las salas de videoconferencia deben ser reservadas a través de los canales*

establecidos para su solicitud.

## Lineamientos

- *Tecnología, tiene bajo su responsabilidad suministrar la ayuda en lo que se refiere a configuración de las aplicaciones y servicios autorizados por la organización.*
- *Soporte requerido sobre dispositivos móviles es responsabilidad exclusiva del colaborador.*
- *Si el colaborador desea un equipo (Dispositivo móvil) diferente al asignado por la organización deberá asumir el costo del equipo de acuerdo con las condiciones pactadas con el operador.*
- *El colaborador que cuente con servicio de telefonía celular asignado por la organización debe respetar el valor del plan establecido y atender los criterios de racionalidad y disciplina en el uso del servicio.*
- *En el caso de pérdida, hurto, daño o deterioro del equipo de cómputo y/o dispositivos móviles su reposición, reparación o mantenimiento estará a cargo de la organización, si este fue asignado por ella. Así mismo, el colaborador debe notificar la pérdida o mal estado en un término no superior a 48 horas.*
- *El colaborador que se retire de la organización, si desea continuar con la misma línea telefónica, debe solicitarlo al equipo de Tecnología para proceder con el trámite de cesión de la línea por parte de la organización a nombre del colaborador, así mismo los planes serán sujetos a las tarifas comerciales del operador móvil.*
- *La asignación del servicio de roaming se realiza de acuerdo con la aprobación del líder del equipo respectivo.*

### 3.5 Gestión de servicios TIC

*Tecnología, promueve la adopción de un enfoque basado en procesos integrados, preservando los principios empresariales, de modo que se entreguen servicios oportunos, efectivos, eficientes y funcionales.*

### 3.6 Manejo y protección de la información

- *Se deben conservar registros de las actividades, de las excepciones o incidentes de información de los clientes, incluyendo administradores y operadores, y mantenerlos durante un período acordado para ayudar en investigaciones futuras o para el seguimiento y monitoreo del control de acceso a los sistemas.*

*En la medida de lo posible se incluirá como mínimo en los registros:*

- *Identificadores de clientes.*
- *Registro de intentos de acceso a los recursos y a los datos exitosos y rechazados.*
- *Cambios en la configuración del sistema.*
- *Uso de privilegios.*
- *Uso de dispositivos y aplicaciones del sistema.*
- *Alarmas por el sistema de control de acceso.*
- *Activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de detección de intrusión.*

**Lineamientos** • Cambios o intentos de cambios en las posiciones y en los controles de seguridad del sistema.

- La frecuencia con que se revisan los resultados de las actividades de seguimiento dependerá de la información y criticidad de los sistemas.
- Las copias de seguridad de la información y de software corporativo se deben realizar periódicamente, considerando lo siguiente:
  - Establecer registros precisos y completos de las copias de seguridad y procedimientos de recuperación documentados.
  - La extensión y frecuencia de las copias de seguridad (totales o incrementales) debe supeditarse a los requisitos de negocio, legales y de seguridad, respecto a la criticidad de la información.
  - Las copias de seguridad deben almacenarse en un lugar diferente y alejado que no esté sujeto a los mismos riesgos de la ubicación principal. Este almacenamiento se hace con un proveedor externo especializado bajo las condiciones ideales para la conservación.
  - La retención de las copias de seguridad será acorde con las necesidades funcionales o regulatorias del aplicativo, soportado en la configuración que se tiene en la herramienta de Backup y el procedimiento de Gestión de Respaldo de la Información que se encuentra publicado en el SGO – Sistema de Gestión Organizacional.

### 3.7 Gestión de servicios a los clientes de las TIC

- Cuando un equipo requiera una solución o componente de software, deberá contactar al líder DevOps del negocio, para definir la prioridad, presupuesto a usar y designar el Product Manager (PM), el equipo de negocio deberá asignar a una persona responsable para acompañar la gestión de dicha iniciativa, quien será el Product Owner (PO).
- Para el manejo y administración de las plataformas tecnológicas (adquisiciones, implementación y mantenimiento) soportados por Tecnología, todos los requerimientos serán canalizados por medio de la herramienta de gestión determinada por la organización.

### 3.8 Relación con infraestructura de terceros

La infraestructura tecnológica de terceros que se utilizan en la organización debe ajustarse a las Políticas de Seguridad, Ciberseguridad y Datos Personales establecidas por la organización.

## 4. Control de cambios

Versión	Fecha	Justificación de la versión
1	27/04/2023	Creación del documento