Versión: 4

Fecha de aprobación: 13/10/2020

Proceso responsable: Tecnología

Aprobado por: Comité Directivo

Tipo de documento: Políticas con sus respectivos estándares

Política de Tecnologías de la Información y las Comunicaciones

El objetivo de la Política TIC es establecer un marco de gobierno para que el uso de las TIC's de la organización, logre satisfacer las necesidades actuales y futuras derivadas de la estrategia del negocio, siguiendo los criterios de innovación, calidad, eficiencia, escalabilidad y de arquitectura empresarial.

La política TIC debe ser revisada por el Líder de Tecnología y aprobada por el Comité Directivo o Líder N1.

Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas para su posterior aprobación por el Líder de Tecnología.

El cumplimiento de la Política TIC es obligatorio para colaboradores de Celsia y sus empresas vinculadas, consultores, contratistas, terceras partes. La organización se reserva el derecho de tomar las medidas correspondientes a las partes interesada que violen estas políticas

Existe un compromiso por parte del Comité Directivo de CELSIA para la difusión, consolidación y cumplimiento de la presente política.

Estándares de la Política de TIC

Esta política aplica a los colaboradores de Celsia y sus empresas vinculadas, contratistas y proveedores, que usen las Tecnologías de Información y la Comunicación de la Organización.

Esta política debe ser revisada como mínimo una vez al año o cuando sea necesario.

Adquisición, implementación y mantenimiento de las TIC

Tecnología, es el responsable de la adquisición, implementación y mantenimiento de todos los servicios y configuración de las Tecnologías de Información y Comunicación (TIC), requeridas para los procesos de la organización, buscando, dentro del marco legal que rija, asegurar la calidad de los servicios entregados y de acuerdo con criterios de innovación, confiabilidad, disponibilidad, seguridad, economía e interoperabilidad, que den soporte a la productividad de los colaboradores en los procesos.

- El proceso de adquisición, implementación y/o desarrollo de cualquier solución de software será realizado exclusivamente por el equipo de Tecnología, siendo este equipo quien defina los lineamientos técnicos de las soluciones de software.
- Cuando un área requiera una solución o componente de software, deberá contactar al equipo de Demanda Tecnológica para el respectivo levantamiento de la necesidad, y asignar a una persona responsable para acompañar la gestión de dicho proyecto.
- El equipo de Tecnología será quien defina los lineamientos técnicos para la adquisición, implementación y/o desarrollo de las soluciones de software.
- El acceso a los archivos del sistema y al código fuente debe ser restringido.
- La actualización del software y las librerías solo pueden ser llevadas a cabo por los administradores, 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.

- Para minimizar los riesgos en el proceso de puesta en producción de los cambios y nuevos desarrollos, así como el impacto por la no disponibilidad de los servicios, se debe 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, dominios y directorios.
    - ✓ La restricción de uso de compiladores, editores y otras herramientas de desarrollo o recursos del sistema en ambientes de producción.
    - ✓ Los sistemas de prueba deben emular al sistema productivo tan real como sea posible.
    - ✓ Los menús 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.

- Las aplicaciones que se desarrollen tanto internamente o por encargo a un proveedor, deben cumplir con los requerimientos de seguridad establecidos por la organización:

    - ✓ Prácticas de desarrollo seguro.
    - ✓ Análisis de riesgos.
    - ✓ La política de Seguridad de la Información, la política para el tratamiento de datos personales y la política de ciberseguridad

- Para el manejo y administración de las plataformas tecnológicas (adquisiciones, implementación y mantenimiento), todos los requerimientos serán canalizados por medio de la herramienta de gestión determinada por la organización.

- Las redes y la infraestructura de apoyo deben ser adecuadamente gestionadas y aseguradas para protegerlas de amenazas y garantizar la seguridad de los sistemas y aplicaciones.

- Se deben implantar controles relacionados con la segmentación, gestión, monitoreo y detección de eventos, para asegurar la información que viaja por las redes.

- La virtualización de escritorios debe garantizar que todos los datos de usuarios se almacenen de una manera central, y que la información no se almacene a nivel local.

- Los proveedores de servicios de virtualización podrán ser utilizados para ambientes de desarrollo y continuidad. Cualquier excepción debe ser autorizada por Tecnología, con base en un análisis de riesgos.

- Se deben establecer proyecciones de capacidad futura y realizar monitoreo al uso de los servicios de red y de los sistemas.

- En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permite la instalación de software con licenciamiento apropiado y acorde con la propiedad intelectual.

- Debe existir un inventario de medios magnéticos y debidamente almacenados de acuerdo con las prescripciones del fabricante para prevenir la pérdida o deterioro de la información, salvaguardando la protección de los medios magnéticos, para prevenir la revelación, modificación, eliminación o destrucción no autorizada, durante el transporte fuera de los límites físicos de la organización, esto se hace por medio de transportes autorizados con soportes debidamente cifrados cuando sean requeridos.

- Todos los medios deben ser etiquetados de acuerdo a la clasificación y manejo de la información establecido por la organización.

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

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

  - ✓ Identificadores de usuarios.
  - ✓ 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.
  - ✓ 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.

- Tecnología es el responsable de definir las necesidades que tiene la compañía respecto a las redes, de la administración de los anchos de banda necesarios para soportar los servicios TIC.

- Cualquier solicitud de servicio que no pueda ser soportada por la infraestructura existente debe negociarse con el área respectiva y seguir los estándares de implementación.

- La asignación de extensiones telefónicas y modificación de categorías de acceso telefónico 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.

- Los servicios de radiocomunicación son de uso exclusivo para la gestión de maniobras sobre la red eléctrica o donde no exista cobertura de otro medio de comunicación.

- El servicio de Telemedida da lectura a los medidores de los clientes regulados, no regulados y puntos de frontera. Las lecturas se harán de forma centralizada.

- Las solicitudes de servicio de telecontrol de las nuevas subestaciones son solicitadas directamente a Tecnología de la Organización. La Mesa de Servicios canalizará los requerimientos o incidentes con el proveedor de outsourcing de telecomunicaciones.

- Todas estas modificaciones deben estar documentados bajo los lineamientos establecidos en el procedimiento de cambios.

Equipos portátiles y dispositivos móviles

Tecnología, establece los requisitos y controles para la conexión de equipos portátiles y los dispositivos móviles a la red de la compañía.

Los colaboradores, consultores, contratistas y terceras partes, podrán hacer uso de los dispositivos móviles, siempre y cuando cumplan con los criterios técnicos, funcionales, de seguridad, regulatorios y económicos establecidos por la organización.

- Los colaboradores, consultores, contratistas y terceras partes, podrán hacer uso de los dispositivos móviles, siempre y cuando cumplan con los criterios técnicos, funcionales, de seguridad, regulatorios y económicos establecidos por la organización.

- La asignación de los equipos y planes de telefonía celular para los colaboradores se realiza de acuerdo con la aprobación del líder del área respectiva.

- Tecnología, tiene bajo su responsabilidad suministrar la ayuda en lo que se refiere a configuración de las aplicaciones y servicios autorizados por la organización, cualquier otro soporte es responsabilidad exclusiva del colaborador.

- Si el colaborador desea un equipo 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, 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.

- Tecnología, tiene bajo su responsabilidad de revisar los consumos de voz y datos de cada colaborador al que se le ha asignado la línea de la organización y aquellos valores que sobrepasan los límites autorizados son deducidos por nómina.

- El colaborador que se retire de la organización, si desea continuar con la misma línea telefónica, debe solicitarlo por escrito al equipo de Tecnología para proceder con el trámite de ceder la línea 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 área respectiva.

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.

Manejo y protección de la información

Todos los colaboradores, consultores, contratistas y terceras partes que manejen información de la organización, están obligados a salvaguardarla en los sitios dispuestos para tal fin, para garantizar la disponibilidad, confidencialidad y respaldo de la misma.

- El uso de recursos compartidos en los equipos de cómputo de los usuarios es una práctica que, aunque puede ser una herramienta útil de trabajo, tiene implícitos riesgos que pueden afectar los principios de confidencialidad integridad y disponibilidad de la información. Por lo tanto, su uso debe ser controlado.

- El usuario que autoriza el acceso a las carpetas y dispone el recurso compartido, es el responsable por las acciones y los accesos sobre la información contenida en dicha carpeta.

- Se debe definir el tipo de acceso y los roles estrictamente necesario sobre la carpeta (Lectura, Escritura, Modificación, Borrado). Además, se debe especificar el límite de tiempo durante el cual estará publicada la información y el recurso compartido en el equipo.

- Para la información confidencial o critica para la compañía, deben utilizarse las carpetas destinadas en el servidor de archivos de usuarios, con el fin de que sea incluida en las copias diarias de respaldo.

- No se debe compartir carpetas a usuarios que no cuenten con software de antivirus corporativo y actualizado.

- Las copias de seguridad de la información y de software se deben realizarse 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. Estas deben almacenarse en armarios que eviten la combustión con acceso restringido.

- ✓ La retención de las copias de seguridad será acorde con las tablas de retención definidas en el Sistema de Gestión Documental o en el Sistema de Gestión de Calidad.

- La organización, en respeto de los principios de libertad de expresión y privacidad de información, podrá denegar todos los servicios asignados por Tecnología.

- La organización puede conservar y revelar contenidos que sean requeridos por la ley o si de buena fe considera que dicha reserva o revelación es necesaria para:

  - ✓ Cumplir con los procesos legales.

  - ✓ Responder a quejas sobre contenido que violen los derechos de terceras personas.

  - ✓ Proteger los derechos, propiedad o seguridad personal de la organización, sus usuarios y el público en general.

  - ✓ La violación de los controles de seguridad o el incumplimiento de las políticas de la organización por parte de los colaboradores dará lugar a la aplicación de medidas administrativas, disciplinarias, civiles o penales a las que haya lugar.

Gestión de servicios a los usuarios de las TIC

La Mesa de Servicios será el único canal por medio del cual se reportará cualquier incidente o requerimiento asociado a las TIC, con el fin de garantizar el seguimiento y entrega oportuna del servicio solicitado, con base en los acuerdos de nivel de servicio ofrecido.

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 de conformidad mínimas establecidas por la organización, aplicables a los activos en alquiler, servicios de hosting de aplicaciones y equipos e infraestructura de telecomunicaciones, y debe ser siempre aprobada por Tecnología.

Gestión del riesgo TIC

Tecnología, debe identificar, calificar, priorizar y realizar el tratamiento de los riesgos tecnológicos, con base en los objetivos de negocio y de acuerdo con la política de gestión de riesgos corporativa y Seguridad de la Información.

Incorporación al cumplimiento regulatorio

Toda solución de servicios o infraestructura tecnológica debe cumplir con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la organización.

Social y Ambiental

El desarrollo de las TIC se orienta bajo los lineamientos de actuación para los colaboradores y el marco de referencia para los demás grupos de interés en materia social y ambiental, garantizando los principios de relacionamiento para la gestión social y considerando la variable ambiental para la toma de decisiones en nuevas inversiones y operación de los activos.

Seguridad de la información

Todos los colaboradores, consultores, contratistas, terceras partes que acceden activos de información de la organización están en la obligación de continuar protegiendo la información por medio del cumplimiento de las políticas de seguridad, durante y aún después de terminar su relación contractual con la organización, de acuerdo con lo pactado entre las partes.

CONTROL DE CAMBIOS

VERSION	FECHA	JUSTIFICACIÓN DE LA VERSIÓN
1	14/08/2013	Creación del documento
2	30/09/2017	Cambio de formato del documento
3	26/07/2019	Actualización del formato del documento Simplificación de la Política.
4	13/10/2020	Ajuste en la descripción del ítem Adquisición, implementación y mantenimiento de las TIC