OBJETIVO	Establecer, promover y mantener los criterios y comportamientos que deben seguir todos los colaboradores, terceros y personas que tengan acceso a los activos de información de TN COLOMBIA, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de esta, dando cumplimiento a las disposiciones legales vigentes, la norma ISO 27001 y las recomendaciones del estándar ISO 27002.
ALCANCE	El presente documento define las políticas específicas, controles y directrices para el Sistema de Gestión de Seguridad de la Información de TN COLOMBIA. Aplica para todos los procesos y activos de información de estos.
REFERENCIA NORMATIVA	• NTC-ISO-IEC-27001:2013. • NTC-ISO-IEC-27002:2013.
TERMINOS Y DEFINICIONES	• **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. • **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. • **Dato personal**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables [Ley 1581 de 2012]. • **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. • **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento de riesgos. • **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. • **Inferencia**: Consiste en la posibilidad de deducir, con una probabilidad significativa, el valor de un atributo al que no se debería tener acceso a través de otros, menos críticos, a los que sí se tiene o se puede tener [Dictamen 05/2014 Grupo de trabajo sobre protección de datos del artículo 29]. • **Integridad:** Propiedad de la información relativa a su exactitud y completitud. • **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. • **Singularización:** Consiste en la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros que identifican a una persona [Dictamen 05/2014 Grupo de trabajo sobre protección de datos del artículo 29].

	• **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua. • **Vinculabilidad:** Consiste en la capacidad de vincular, al menos, dos datos referentes al mismo interesado o grupo de interesados, ya sea a través de una única fuente de datos o varias [Dictamen 05/2014 Grupo de trabajo sobre protección de datos del artículo 29].

1. COMPROMISO DE LA DIRECCIÓN

La alta dirección de TN COLOMBIA aprueba este Manual de Políticas de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de controles, que garanticen la seguridad de la información en la Organización.

2. DIRECTRICES

Todos los colaboradores directos e indirectos de TN COLOMBIA son responsables del cumplimiento de las Políticas Específicas de Seguridad de la Información definidas en este documento, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información en cada una de las actividades realizadas por las áreas y procesos de TN COLOMBIA y que se consolida a través de la aplicación de las políticas específicas y procedimientos definidos en virtud del SGSI.

Toda excepción o desviación a estas políticas debe ser justificada, revisada y autorizada previamente por el Comité de Seguridad de la Información. La excepción que resulte en riesgo significativo o fuera del nivel aceptable para TN COLOMBIA requieren de la aprobación por parte del Comité de Seguridad de la Información y de la Alta Gerencia. En los dos casos se debe mantener el registro de esta actividad.

2.1. 3.1. Principios de Seguridad de la Información

A continuación, se establecen 11 principios de seguridad que soportan el SGSI de TN COLOMBIA:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaboradores, proveedores y terceros de TN COLOMBIA.
- Proteger la información generada, procesada o resguardada por TN COLOMBIA., su infraestructura tecnológica, considerando el riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes).
- Proteger la información creada, procesada, transmitida o resguardada por TN COLOMBIA., con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para esto es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Proteger su información de las amenazas originadas por parte del personal.
- Proteger las instalaciones de procesamiento e infraestructura tecnológica que soporta TN COLOMBIA.
- Controlar la operación de TN COLOMBIA garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar control de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- Garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora continua de su SGSI.
- Garantizar la disponibilidad de TN COLOMBIA y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

3. CONTENIDO

3.1. Organización de la Seguridad de la Información

3.1.1. Dispositivos Móviles

- Se proveerá las condiciones para el manejo de los dispositivos móviles (equipos portátiles, teléfonos inteligentes, entre otros) corporativos que hagan uso de servicios del proceso. Así mismo, velará porque los colaboradores hagan un uso responsable de los servicios y equipos proporcionados por el mismo.
- Se debe investigar y probar las opciones de protección de los dispositivos móviles corporativos, así como la realización de configuraciones iniciales en los dispositivos móviles que hagan uso de los servicios entregados por el mismo.
- Se debe establecer un método de bloqueo para la protección de los equipos portátiles corporativos que serán entregados a los colaboradores.
- Se debe configurar los equipos portátiles para que pasado cinco (5) minutos de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo por usuario y contraseña.
- Se debe garantizar el borrado seguro de los dispositivos móviles cuando se desvincule un colaborador o los dispositivos sean dados de baja.
- Se debe instalar un software de antivirus en los dispositivos móviles corporativos usados para la operación de TN COLOMBIA.
- Los colaboradores deben evitar usar los dispositivos móviles corporativos en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los colaboradores deben evitar hacer uso de redes inalámbricas de uso público a menos que sea estrictamente necesario, así como deben desactivar las conexiones de Bluetooth o infrarrojos en los dispositivos móviles corporativos asignados.
- Los colaboradores deben evitar almacenar videos, fotografías o información personal en los dispositivos móviles corporativos asignados. En caso de que se almacene información personal, como videos, fotografías o información personal en los equipos de cómputo corporativos, TN COLOMBIA no asume responsabilidad por eventos o incidentes relacionados con esta información.
- La utilización de WhatsApp web y redes sociales corporativas se autoriza únicamente en los celulares de propiedad de TN COLOMBIA y exclusivamente por parte de las personas autorizadas o áreas designadas para ello.

- El uso de los equipos de cómputo portátiles fuera de las instalaciones de TN COLOMBIA únicamente se permitirá a usuarios autorizados por el Líder del proceso, y estos deben estar protegidos mediante el uso de los siguientes controles tecnológicos: Antivirus, Firewall, VPN, entre otros.

3.1.2. Trabajo remoto

- Se deben analizar y aprobar los métodos de conexión remota a las plataformas tecnológicas de TN COLOMBIA.
- Se debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia las plataformas tecnológicas de TN COLOMBIA.
- Se debe restringir las conexiones remotas a los recursos de las plataformas tecnológicas; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Se debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de las plataformas tecnológicas de TN COLOMBIA.
- Los colaboradores que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de las plataformas tecnológicas de TN COLOMBIA y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Los colaboradores únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

En caso de formalizarse y definirse la modalidad de trabajo remoto, se deberán tener en cuenta:

- El entorno físico de trabajo remoto propuesto.
- Los requisitos de seguridad de las comunicaciones, teniendo en cuenta que el acceso remoto deberá ser por VPN, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación.
- La amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo alojamiento, por ejemplo, familia y amigos.
- El uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica.
- Acuerdos para evitar disputas acerca de derechos de propiedad intelectual sobre la información, datos y demás activos propiedad de TN COLOMBIA. que se realicen en equipos de propiedad privada.
- La propiedad intelectual desarrollada o concebida mientras el colaborador este vinculado con TN COLOMBIA y se encuentre en sitios de trabajo alternos, es propiedad exclusiva de TN COLOMBIA.
- Requisitos de firewall y de protección contra software malicioso.

Las directrices y acuerdos que se consideren deberían incluir:

- El suministro de equipo adecuado y de muebles de almacenamiento para las actividades de trabajo remoto.
- El suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto.
- Las reglas, responsabilidades y la orientación sobre el acceso de la familia y los visitantes a los equipos y a la información;
- El suministro de soporte y mantenimiento del hardware y el software.
- Los procedimientos para copias de respaldo y continuidad del negocio
- Auditoría y seguimiento de la seguridad.
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades de bajo la modalidad de trabajo remoto finalicen.

3.1.3. Seguridad de la información en la gestión de proyectos:

- Los riesgos de seguridad de la información se incluyen como parte del análisis de riesgos del proyecto, el cual se lleva a cabo en una etapa temprana para identificar los controles necesarios.
- Se garantiza que los procesos de seguridad de la información son parte de todas las fases de las metodologías aplicadas a los proyectos independientemente del tipo de proyecto.

3.2. Gestión Humana

- Todos los colaboradores de TN COLOMBIA y terceros que tengan la posibilidad de acceder a la información y a la infraestructura para su procesamiento son responsables de conocer y cumplir las políticas y procedimientos establecidos por el SGSI. De igual forma, son responsables de reportar por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.
- Todos los colaboradores, deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de TN COLOMBIA.
- Toda vinculación laboral realizada por TN COLOMBIA se rige por las leyes de la República de Colombia y por lo dispuesto en el Código Sustantivo del Trabajo.
- Todo colaborador contratado es seleccionado adecuadamente, de acuerdo con los requisitos de cada cargo y el procedimiento dictado por Gestión Humana.
- Todos los colaboradores y terceros deben acoger las políticas de Seguridad de la Información, así como los términos de uso adecuado de los recursos de información que le son entregados, teniendo en cuenta que estos términos y responsabilidades son extensibles fuera de TN COLOMBIA.
- Todos los colaboradores y terceros que tengan acceso a información confidencial o a la infraestructura tecnológica que contenga este tipo de información, deben firmar, previo a la entrega del acceso, un acuerdo de confidencialidad y no divulgación, en el que se especifique el período por el cual se debe mantener el acuerdo y las acciones que se toman cuando se incumpla este requisito.

- Se debe asegurar que todos los colaboradores que tengan definidas responsabilidades de Seguridad de la Información son competentes para desempeñar sus funciones y que cuentan con la capacitación y entrenamiento requerido para ello.
- Gestión de Talento Humano en conjunto con TN COLOMBIA, son los responsables del proceso de terminación de labores y aseguran que todos los activos propios del proceso sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, de acuerdo con el procedimiento dictado por Gestión de Talento Humano.
- En caso de que un colaborador de TN COLOMBIA tenga un cambio de funciones, se debe seguir el procedimiento dictado por Gestión de Talento Humano, asegurando la entrega de activos, el retiro de los accesos físicos y lógicos, la disposición segura de los activos y la posterior entrega de estos de acuerdo con su nuevo rol.
- El incumplimiento de lo establecido en el presente documento por parte de los colaboradores de TN COLOMBIA aplicará procesos disciplinarios internos.

3.3. Gestión de Activos de Información

3.3.1. Inventario de Activos

- Al menos una vez al año, El Líder del área o proceso, identificará y/o actualizará los activos de información (hardware, software, servicios, conocimiento, entre otros) por medio de un inventario de activos en donde se define como mínimo establecer la ubicación, propietario (responsable), custodio, entre otros.
- El Líder del área o proceso, gestionara la adquisición de nuevos activos de información y deberá actualizar el inventario de activos del proceso para garantizar que los activos más relevantes del mismo sean identificados y valorados.

3.3.2. Asignación de equipos

- El Líder del área de Gestión de Tecnologías de la Información o quien haga sus veces, controla la asignación de equipos tecnológicos. Cuando un colaborador es contratado, el jefe Inmediato realiza la solicitud de asignación de equipos de cómputo por medio de un correo electrónico a la mesa de ayuda.
- La entrega del equipo se realiza dejando evidencia en acta de las condiciones en que se entrega este.

3.3.3. Uso aceptable de Activos

- Todos los colaboradores deben etiquetar la información, y darle un manejo adecuado según su clasificación, siguiendo las directrices del Manual y Procedimiento para la Gestión de activos de TN COLOMBIA.
- Los Colaboradores, deben reportar los eventos de seguridad de la información identificados, de acuerdo con el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad del área de Gestión de Tecnologías de la Información, por tanto, se debe realizar una solicitud para la ejecución de estas labores.
- Debe respetarse y no modificarse la configuración de hardware y software establecido por TN COLOMBIA.
- Durante la permanencia en las instalaciones de TN COLOMBIA, los equipos de cómputo externos deben estar conectados únicamente a la red de datos de invitados.
- Los equipos de cómputo (CPU y monitor), servidores, teléfonos y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados.
- La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de TN COLOMBIA y que no son propiedad de esta, serán responsabilidad única y exclusiva de sus propietarios. TN COLOMBIA no se responsabilizan por estos equipos en ningún caso.
- En TN COLOMBIA NO está permitido que los colaboradores accedan a cualquier página o dirección web que contenga material pornográfico en cualquiera de sus variantes, o bien, páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de TN COLOMBIA, tales como violencia, terrorismo, grupos al margen de la ley, discriminación, entre otras.
- No está permitido el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.
- Todo Colaborador es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta corporativa.
- TN COLOMBIA provee a todos los colaboradores un correo electrónico institucional en el dominio **@tncolombia.com.co**, para el ejercicio de sus labores.
- La cuenta de correo electrónico institucional es personal e intransferible y, por ende, los usuarios son completamente responsables de todas las actividades realizadas con sus credenciales de acceso y el buzón asociado al correo de TN COLOMBIA.
- El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de TN COLOMBIA, es decir, que debe ser usado para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo asignadas.
- Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas, datos e información de TN COLOMBIA.
- El usuario debe notificar correos sospechosos maliciosos, según lo indica el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

3.3.4. Retiro de equipos

- Para aquellos casos en donde sea necesario el retiro de equipos de cómputo de las instalaciones de TN COLOMBIA, por parte de los colaboradores, se debe gestionar la autorización con su jefe inmediato y se deja registro en acta (en caso de trabajo en casa no es necesario dejar registro en acta).

3.3.5. Devolución de equipos y disposición segura

Cuando un colaborador devuelve el equipo de cómputo asignado por terminación de contrato o cuando se va a dar de baja un equipo, el encargado de gestionar los equipos evalúa si el activo contiene información confidencial o privada para TN COLOMBIA, con el fin de disponer de forma segura:

- Realización de copia de respaldo a la información.
- Formatear o sobrescribir los equipos de cómputo.
- Control de revisión de software instalado y monitoreo de software en los equipos de cómputo asignados a los colaboradores.

Cuando un colaborador termina su relación contractual con la empresa, debe contar con el Formato de devolución de activos para dar paz y salvo a su liquidación.

3.3.6. Gestión de medios removibles

- Las unidades de medios removibles deben estar deshabilitadas en los servidores y equipos de cómputo. En caso de ser necesario el uso de medios removibles, se debe hacer seguimiento a la transferencia de información a estos medios por medio del registro de eventos de los equipos de cómputo; adicionalmente, debe existir un registro de la solicitud del desbloqueo de puertos y autorización por parte del líder de proceso. Esta autorización debe indicar la duración específica durante la cual los colaboradores están autorizados para utilizar las unidades de medios removibles en sus equipos de cómputo.
- El almacenamiento, etiquetado y eliminación de los medios de almacenamiento removibles, debe estar de acuerdo con el esquema de clasificación y seguir los procedimientos relacionados con la gestión de activos de información.
- Si ya no se requiere, el contenido de cualquier medio removible que se vaya a retirar de la organización se debería remover de forma que no sea recuperable.

3.4. Control de Acceso

3.4.1. Control de acceso lógico

- La autorización para el acceso a los sistemas de información de TN COLOMBIA debe ser definida y aprobada por líder de proceso, y se debe otorgar de acuerdo con los controles y privilegios de acceso a los colaboradores y terceros, según el rol que vayan a desempeñar.
- Se debe asegurar que los accesos a los servicios y aplicativos de TN COLOMBIA cuenten con métodos de autenticación que evite accesos no autorizados.
- Los derechos de acceso privilegiados se deben asignar a los colaboradores con base en la necesidad de uso y caso por caso. Adicionalmente, los derechos de acceso

privilegiado se deben asignar a una identificación de usuario diferente de la usada para las actividades regulares de TN COLOMBIA.

- Los accesos a los sistemas de información y equipos de cómputo de TN COLOMBIA requeridos por los proveedores deben ser solicitados de manera formal únicamente al Líder del proceso o quien haga sus veces.
- Se debe realizar la inactivación del usuario, al momento de finalizar el contrato o al concluir con las actividades requeridas, todo acceso a los sistemas de información de TN COLOMBIA otorgado a colaboradores, proveedores o entes de control.
- Cualquier actividad realizada por un colaborador o tercero en los sistemas de información de TN COLOMBIA, debe ser monitoreada. En el caso que se identifiquen riesgos de seguridad sobre la información, inmediatamente será revocada su autorización y el sistema será bloqueado.
- El acceso remoto realizado a los servicios de TN COLOMBIA deberá ejecutarse a través de la VPN.
- Se debe evitar llevar un registro (por ejemplo, en papel o en notas de escritorio lógico) de información de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, un software para la gestión de contraseña autorizado por TN COLOMBIA).
- Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
- Se deben asegurar restringir el acceso a los códigos fuente de los programas, con controles de cifrado, ofuscación de código fuente, entre otros.
- Se definen lineamientos para la configuración de contraseñas que aplican sobre las plataformas tecnológicas, los servicios de red y los sistemas de información de TN COLOMBIA; dichos lineamientos consideran aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros, así:
  - La contraseña debe tener una longitud mínima de 10 caracteres.
  - Al momento de crearla debe intentarse combinar letras mayúsculas y minúsculas, números y caracteres especiales (por ejemplo: @, $, &,*).
  - Debe cambiarse, dependiendo de la criticidad del recurso al que da acceso, cada 30 días calendario.
  - No debe tenerse la misma contraseña todas las plataformas tecnológicas, los servicios de red y los sistemas de información. Es altamente recomendable que varíe de un sistema a otro.
  - Se debe evitar crear contraseñas con el nombre del usuario de la cuenta o con información personal obvia como nombre del cónyuge, hijos, fechas de cumpleaños, entre otros. Tampoco debe tener una secuencia previsible de letras o números como abcd o 1234, o una simple palabra en cualquier idioma.

3.4.2. El Control de acceso físico

- Está prohibido la toma de imágenes fotográficas y videos en las instalaciones de TN COLOMBIA.

- Todas las áreas destinadas al procesamiento o almacenamiento de información confidencial, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones de TN COLOMBIA, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.
- El datacenter, centros de cómputo, cableado y cuartos técnicos deben estar equipados con mecanismos que garanticen el cumplimiento de los requisitos ambientales (como temperatura, humedad, etc.) establecidos por los fabricantes de los equipos alojados en ellos. Además, es crucial que estos mecanismos puedan responder de manera efectiva ante situaciones de emergencia, como incendios e inundaciones.
- Los equipos que hacen parte de la infraestructura tecnológica de TN COLOMBIA, tales como, servidores, equipos de comunicaciones, centros de cableado, UPS, aires acondicionados, así como estaciones de trabajo y dispositivos de almacenamiento que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo entre otros.
- TN COLOMBIA debe proveer suministros y equipamiento de soporte como electricidad, aire acondicionado y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de energía, evitando así la pérdida o corrupción de información. Estos suministros deben revisados periódicamente por el área de tecnología o quien haga sus veces, para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.
- Las instalaciones de procesamiento de la información se encuentran físicamente protegidas adecuadamente contra acceso no autorizado; las puertas permanecen cerradas cuando no hay supervisión del personal autorizado para ingresar a las mismas. Adicionalmente, se cuenta con un sistema CCTV para dejar registro de las personas que ingresan y se retiran de TN COLOMBIA.
- Todo ingreso de personal externo a TN COLOMBIA debe ser registrado, al igual que los equipos portátiles externos ingresados. Para el ingreso de personal interno se debe dejar registro por medio del control biométrico instalado en la entrada en el centro de cableado y UPS.
- Los visitantes y proveedores de TN COLOMBIA deben acatar los controles de acceso definido en el presente documento.
- El ingreso al centro de datos de TN COLOMBIA solo debe permitirse al personal autorizado, al igual que la manipulación de las llaves que permiten su acceso.

3.5. Criptografía y Gestión de Llaves

- Se deben establecer procesos para la gestión apropiada de las llaves en todas sus etapas: generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción. De este modo se protegen contra modificación, pérdida y divulgación de información no autorizada.
- Se debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información confidencial cuente con mecanismos de cifrado de datos.
- La administración de claves criptográficas y certificados digitales estará a cargo del área Gestión de Tecnologías de la Información. Sin embargo, la administración de tokens bancarios será a cargo del personal autorizado por las áreas Administrativas o a quien esta asigne la responsabilidad.
- En el momento que se sospeche que una llave criptográfica o mecanismo de cifrado ha perdido su confidencialidad o está comprometida la misma, se debe reportar como evento de seguridad de la información de acuerdo con los procedimientos internos de TN COLOMBIA.

3.6. Seguridad Física y del Entorno

3.6.1. Escritorio limpio y pantalla limpia

- Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los colaboradores de TN COLOMBIA deben mantener la información privada o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CD´s, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información confidencial que se envía a las impresoras sea recogida manera inmediata.
- Todos los colaboradores de TN COLOMBIA son responsables de bloquear la sesión de su equipo de cómputo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados,
- La información clasificada como altamente confidencial no debe ser nunca enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión.
- El escritorio lógico debe estar libre de información confidencial.

3.6.2. Protección de los equipos

- Los equipos que hacen parte de la infraestructura tecnológica de TN COLOMBIA, tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las

dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

- Se debe establecer y ejecutar un plan semestral de mantenimiento preventivo a la infraestructura tecnológica de hardware y de software mensual.

3.6.3. Seguridad de equipos y medios de información fuera de las instalaciones

Independientemente del propietario, todos los colaboradores son responsables de velar por la seguridad de los equipos de TN COLOMBIA que se encuentren fuera de las instalaciones de la organización, siguiendo las siguientes directrices:

- En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de TN COLOMBIA, el colaborador deberá informar inmediatamente al jefe inmediato para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

3.7. Seguridad En Las Operaciones

3.7.1. Gestión de Cambios

- Todo cambio que se realice sobre la infraestructura tecnológica de TN COLOMBIA, para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar riesgos asociados que pueden afectar la operación del negocio de acuerdo con los lineamientos de gestión de cambios.
- El procedimiento de gestión de cambios obliga a especificar como mínimo la identificación, justificación y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica, el alcance, autorización, el plan de trabajo para la definición de pruebas funcionales, responsabilidades definidas, la evaluación apropiada sobre el impacto potencial que estos puedan generar, un plan alternativo para abortar cambios no satisfactorios (Rollback) y cualquier otro aspecto que se considere importante por los responsables del cambio.

3.7.2. Gestión de la capacidad

- TN COLOMBIA mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.
- Periódicamente, se realizarán mediciones de las variables críticas de operación de la infraestructura tecnológica con el objetivo de verificar el estado y uso de los recursos. De esta forma, es posible definir proyecciones de crecimiento que aseguren la integridad de procesamiento y disponibilidad de la infraestructura.
- Los resultados de dichas mediciones serán analizados y presentados a la Dirección y el área financiera, para el caso de ser necesaria la adquisición de nuevos recursos o elementos para soportar la demanda, se proceda a planificar la consecución de dichos elementos.

3.7.3. Protección contra software malicioso

TN COLOMBIA establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red institucional. Así mismo define que NO está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por almacenamiento físico o virtual.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, y/o que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo o que no hayan sido previamente autorizados por el proceso de Gestión de Tecnologías de la Información para ser usados con fines corporativos.

3.7.4. Vulnerabilidades técnicas

- Se debe elaborar y ejecutar un plan de pruebas de vulnerabilidades para las plataformas críticas de TN COLOMBIA, cuya viabilidad técnica y de administración lo permita.
- Los correctivos que requieran ser aplicados en las plataformas tecnológicas de TN COLOMBIA, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de Gestión de Tecnologías de la Información o quien haga sus veces.
- Gestión de Tecnologías de la Información o quien haga sus veces, es responsable de verificar de manera periódica (al menos una vez al año) la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de TN COLOMBIA.

- Se debe elaborar y ejecutar por lo menos una vez al año el plan de pruebas de vulnerabilidades para las plataformas críticas de TN COLOMBIA, cuya viabilidad técnica y de administración lo permita.
- Se deben establecer mecanismos, procesos o procedimientos que permitan prevenir la fuga de datos mediante sistemas, redes o cualquier otro dispositivo que procese, almacene o transmita información confidencial propiedad de TN COLOMBIA.

3.7.5. Copias de respaldo (Backups)

- Se debe garantizar la realización de copias de respaldo de los datos almacenados en los repositorios de información autorizados por TN COLOMBIA, así como de la base de datos, código fuente si aplica, y otros datos relevantes, de acuerdo con lo establecido en el procedimiento de gestión de copias de respaldo.
- Semestralmente se debe realizar pruebas de restauración de las copias de respaldo de acuerdo con lo establecido en este documento permitiendo dejar evidencia documentada de las pruebas realizadas.
- Se debe establecer tiempos de retención de las copias de respaldo generadas, para no afectar la capacidad de la infraestructura tecnológica y generar gastos innecesarios.

3.7.6. Protección de registros

- TN COLOMBIA se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requerimientos normativos, legales o regulatorios de pérdida, destrucción o falsificación. De igual forma, y cumpliendo la legislación colombiana vigente, TN COLOMBIA establece que la información personal de los colaboradores, contratistas y terceros es de carácter confidencial, por lo cual se implementarán los controles necesarios para su protección y en ningún momento puede ser divulgada a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la normatividad lo permita.
- TN COLOMBIA asegura que sus procesos velan por que los registros impresos estén protegidos de la humedad, polvo, roedores y de cualquier daño o pérdida, así como también que los registros almacenados en medios magnéticos son protegidos de la humedad, calor, polvo, virus informático, cambios de voltaje y borrado accidental, con el fin de proteger los registros magnéticos se realizan copias de seguridad de dicha información.
- Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, todos los relojes de los sistemas informáticos de TN COLOMBIA deben estar sincronizados con una única fuente de información (hora legal colombiana).
- Las aplicaciones que hacen parte de la infraestructura para el procesamiento de información, comunicaciones y seguridad de TN COLOMBIA deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

- Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes para la seguridad de la información, se deben producir, almacenar, proteger y analizar; de acuerdo con el nivel de importancia o criticidad para TN COLOMBIA, por lo que Gestión de Tecnologías de la Información o quien haga sus veces, establecerá los tiempos de retención de dichos registros, la forma de almacenamiento y los demás controles de seguridad que apliquen a los mismos.
- TN COLOMBIA definirá directrices, formatos, procesos y/o procedimientos para la adecuada protección de registros físicos durante todo su ciclo de vida, garantizando la seguridad de la información de acuerdo con su nivel de clasificación.

3.7.7. Auditorías de sistemas de información

Para la ejecución de una auditoría a los sistemas de información, se deben tener en cuenta las siguientes consideraciones:

- Los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con el líder de proceso correspondiente.
- El alcance de las pruebas técnicas de auditoría se debería acordar y controlar.
- Las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deberían realizar fuera de horas laborales.
- Se debería hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.

3.8. Seguridad de las Comunicaciones

3.8.1. Seguridad en redes

TN COLOMBIA definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la organización y controlar el acceso no autorizado, mediante la segmentación de redes y monitoreo considerando la ejecución de las siguientes acciones:

- Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas y controles específicos para filtrado web.
- Controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas.
- Toda información confidencial que viaje por las redes de comunicación de TN COLOMBIA debe estar cifrada.
- Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones; y se deben adoptar medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

- Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) que afecte tanto las redes corporativas como los sistemas de información de TN COLOMBIA, debe ser catalogada como ilícita y se podrá iniciar los procesos disciplinarios o legales a que haya lugar.

3.8.2. Transferencia de información

- TN COLOMBIA asegurará la protección de la información en el momento de ser transferida o intercambiada con otras Entidades y establecerá los controles necesarios para el intercambio de información; así mismo, se establecerán acuerdos de confidencialidad o de Intercambio de Información con los proveedores que se realice dicho intercambio. Adicionalmente, velará por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información.
- TN COLOMBIA debe hacer firmar acuerdos de confidencialidad y de Intercambio de información con proveedores, incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir:

    - La prohibición de divulgar la información entregada por parte de TN COLOMBIA a los terceros con quienes se establecen estos acuerdos.
    - La destrucción de dicha información una vez cumpla su cometido.

- Se debe velar porque el intercambio de información con Entidades externas se realice en cumplimiento de este documento, los acuerdos de intercambio de Información y el procedimiento definido para dicho intercambio de información.
- Los colaboradores de TN COLOMBIA deben utilizar únicamente el correo electrónico corporativo y el correo certificado como medios de transferencia de información, es decir, para el envío o recepción de información propiedad de TN COLOMBIA.
- Los colaboradores de TN COLOMBIA deben evitar enviar información confidencial a través de correo electrónico, pero en el caso de que sea estrictamente necesario se debe cifrar la información enviada.

3.9. Relación con Proveedores

- Todos los proveedores y contratistas que manipulen información de TN COLOMBIA en el desarrollo de sus funciones deberán firmar un acuerdo de confidencialidad de la información, donde se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso.
- Se deben establecer y acordar los requisitos de seguridad de la información con cada proveedor en función del tipo de relación que se tenga con este y el nivel de acceso a los activos de información de TN COLOMBIA.
- Los accesos a los sistemas de información y equipos de cómputo de TN COLOMBIA requeridos por los proveedores deben ser autorizados de manera formal.

- Todas las actividades realizadas en los sistemas de información de TN COLOMBIA, durante la ejecución del contrato, por parte de proveedores, deben ser monitoreadas por TN COLOMBIA. En caso de evidenciar abuso en los accesos se debe informar inmediatamente al área o proceso responsable de la supervisión del proveedor y reportar el caso como un evento de seguridad de la información, de acuerdo con el procedimiento diseñado para tal fin.
- Se debe monitorear periódicamente, el cumplimiento de los acuerdos de niveles de servicio, acuerdos de confidencialidad, acuerdos de intercambio de información y los requisitos de seguridad de la información.
- Se debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.
- Se debe identificar y mitigar los riesgos relacionados con proveedores que tengan acceso a los sistemas de información y las plataformas tecnológicas de TN COLOMBIA. y deben ser monitoreados por el supervisor del contrato durante la vigencia de la relación contractual. Así como los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.
- TN COLOMBIA debe divulgar las políticas, normas y procedimientos de seguridad de la información a sus proveedores de servicio y realizar evaluación de proveedores para garantizar que las estén cumpliendo.
- Los proveedores deben reportar los eventos de seguridad de la información que se detecten durante la relación contractual, sobre los activos de información de TN COLOMBIA.
- El proveedor que suministre servicios de TI deberá:

    - Contar con un Plan de Continuidad del Negocio; además si TN COLOMBIA requiere el envío y resultado de las pruebas de este plan, debe ser suministrado sin inconveniente por el proveedor.
    - Informar a TN COLOMBIA los datos del personal de contacto y horarios de disponibilidad de los responsables que durante la vigencia del contrato atenderán situaciones críticas y de indisponibilidad de los servicios suministrados. Además, deberá garantizar que dicho recurso esté disponible para la atención y cuente con los conocimientos técnicos requeridos para atender las situaciones que se presenten.

- TN COLOMBIA monitorea, revisa, evalúa y gestiona regularmente el cambio de prácticas de seguridad de la información de los proveedores y la prestación de los servicios, a través de la supervisión de los contratos y el encargado de seguridad de la información, en caso de ser necesario.
- Se deberán gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC, por lo que TN COLOMBIA. define e implementa procesos y procedimientos que permitan realizar dicha gestión.

- Dentro de los acuerdos con proveedores se deberá definir las responsabilidades concretas de ambas partes.

- Cuando la organización lo determine, establecerá acuerdos de niveles de servicio (ANS).
- Se debe monitorear periódicamente, el cumplimiento de los acuerdos de niveles de servicio, acuerdos de confidencialidad, acuerdos de intercambio de información y los requisitos de seguridad de la información.
- Cuando la organización así lo determine exigirá a sus proveedores certificaciones que garanticen la calidad en materia de seguridad de ciertos servicios contratados de especial criticidad.
- Proveedores y terceros solo deben tener acceso a la información, sistemas de información o instalaciones que son indispensables para el cumplimiento de su objeto contractual.
- Cuando la organización lo determine se deberán incluir cláusulas a fin de que los proveedores y sus terceros cumplan con la reglamentación en materia de derechos de autor y propiedad intelectual, incluido, pero no limitado al uso de información y software.
- No está autorizada la ejecución de cambios sobre la infraestructura de información y comunicaciones de TN COLOMBIA S.A.S. sin contar con la autorización formal y expresa de la organización.
- No está autorizada la modificación o desactivación de los controles de seguridad instalados en los componentes de información y tecnología de TN COLOMBIA S.A.S sin contar con autorización del área de Infraestructura Tecnológica.
- El ingreso de personas a las instalaciones de la organización se realizará mediante controles de acceso que permitan registrar la fecha y hora de dicho ingreso.
- Los equipos de cómputo y de comunicaciones que no sean propiedad de la organización, deberán registrarse antes de su ingreso a las instalaciones de la compañía, indicando la fecha, hora de entrada, hora de salida, nombre y apellido, marca, serial y firma.
- Ningún equipo de cómputo o comunicaciones podrá salir de la organización sin que exista una autorización.

3.10. Incidentes de Seguridad de la Información

Toda violación de estas políticas se deberá notificar inmediatamente través de la cuenta designada para esta gestión, de modo que se pueda resolver debidamente el asunto. Se busca asegurar que todos comprendan y respeten las políticas con el fin de reducir al mínimo el riesgo, protegiendo a todas las personas, así como al TN COLOMBIA. Se deberán notificar situaciones tales como:

- Personas ajenas TN COLOMBIA en oficinas y centros de cómputo
- Correos con virus
- Mala utilización de recursos
- Uso ilegal del software
- Mal uso de información corporativa
- Alteración de información, entre otros.

Lo anterior, de acuerdo con los procedimientos definidos por TN COLOMBIA en este asunto.

3.11. Continuidad de la seguridad de la información ante un evento de contingencia

TN COLOMBIA deben implementar los mecanismos para que los controles definidos para proteger la confidencialidad, integridad y disponibilidad de la información se mantengan cuando se activen las estrategias de continuidad y esto se logra a través de los siguientes lineamientos:

- Los controles criptográficos para proteger la confidencialidad y la integridad deben ser implementados en las copias de respaldo y los sistemas redundantes.
- El registro de acciones y operaciones debe mantenerse bajo las mismas condiciones de los sistemas principales en los sistemas redundantes, que se activen en caso de una contingencia.
- El control de acceso debe mantener las restricciones y privilegios en los sistemas redundantes y para las copias de respaldo, acorde con lo establecido por el propietario de la información.
- TN COLOMBIA debe verificar periódicamente la efectividad de los controles establecidos e implementados para dar continuidad a la seguridad de la información durante situaciones adversas.
- TN COLOMBIA junto a la Dirección de TI, debe asegurar que las instalaciones de procesamiento de información cuentan con redundancia suficiente para cumplir los requisitos de la disponibilidad.

3.12. Cumplimiento

- Se debe cumplir con los requisitos legales internos y externos aplicables a la Seguridad y Privacidad de la Información, tales como: Ley de Delitos Informático, Ley de Derechos de Autor, Ley de Protección de Datos Personales, los tiempos de retención de registros, el uso autorizado de recursos de procesamiento, el uso de algoritmos criptográficos fuertes, la recolección de evidencias y la realización de auditorías.
- TN COLOMBIA se regirá por la legislación vigente para el uso de controles criptográficos, según aplique.

3.12.1. Propiedad intelectual

- Se establece que el tratamiento de información externa debe presentar conformidad con los derechos de autor y las leyes nacionales e internacionales que regulen la propiedad intelectual de los mismos.

- NO está permitida la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica.

3.12.2. Privacidad y protección de información de datos personales

TN COLOMBIA será el responsable del tratamiento de los Datos Personales, tal y como este término se define en la Ley 1581 de 2012, respeta la privacidad de cada uno de los titulares que le suministren sus Datos Personales a través de los diferentes puntos de recolección y captura de dicha información.

3.12.3. Revisiones de seguridad de la información

- El líder del proceso debe revisar con regularidad (al menos anualmente) el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, los requisitos de seguridad de la información definidos en las políticas, normas y otras reglamentaciones aplicables.

3.13. Política de Desarrollo Seguro.

El área de Gestión de Desarrollo es el responsable de planificar, desarrollar y ejecutar las actividades relacionadas con desarrollos y actualizaciones de software. Además, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los entornos de producción.

3.13.1. Lineamientos de seguridad para desarrolladores

- Son los responsables de definir y estandarizar el ciclo de vida y los criterios de desarrollo seguro.
- Toda modificación de software bien sea por actualizaciones o modificaciones, debe ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.
- Se deben planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos-instalación, y criterios de aceptación del cambio.
- Para propósitos de desarrollo y pruebas de software, se deben generar datos de prueba que no guarden relación con los que se encuentran en el ambiente de producción.
- Los desarrolladores de TN COLOMBIA y terceros no deben tener acceso a información de producción.

- Cualquier cambio que se ejecute en el ambiente productivo, debe pasar por un control de cambios en donde se evalúen los riesgos de este.
- Se debe establecer un acuerdo previo con desarrolladores y fábricas de software, el cual debe establecer la protección de la propiedad intelectual y el aseguramiento de los niveles de confidencialidad de la información gestionada en los proyectos de desarrollo.
- Se debe establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, que sean publicadas por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido.
- Cada desarrollador debe acatarse a las normas de seguridad, clean code, buenas prácticas y lineamientos de desarrollo seguro definidos por el área.

4. CONTROL DE VERSIONES

VERSIÓN	REVISÓ	FECHA DE REVISIÓN	APROBÓ	FECHA DE APROBACIÓN	REFERENCIA DEL CAMBIO
01	Alejandro Urdaneta/Gerente Ejecutivo	16/09/2021	Paul Suárez / Jefe del SIG	16/09/2021	Creación del documento.
02	Diana Amórtegui/ Oficial de Seguridad de la Información	11/09/2024	Comité de Seguridad de la Información	19/09/2024	Revisión anual, ajuste de redacción, inclusión del numeral 2.12.3., fortalecimiento de políticas de desarrollo seguro y de relación con proveedores.