telepacífico

**SOCIEDAD TELEVISION DEL PACÍFICO LTDA - TELEPACÍFICO**
**RESOLUCIÓN No. 209**
**Junio 30 de 2017**

**"POR MEDIO DEL CUAL SE ADOPTA LA POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA SOCIEDAD TELEVISIÓN DEL PACIFICO LTDA. – TELEPACÍFICO."**

El suscrito Gerente de Sociedad Televisión del Pacífico Limitada - TELEPACIFICO en uso de sus atribuciones legales y estatutarias y,

**CONSIDERANDO**

Que la Sociedad Televisión del Pacífico Ltda. – TELEPACÍFICO, es una sociedad organizada como Empresa Industrial y Comercial del Estado del Orden Departamental, vinculada a la Autoridad Nacional de Televisión – ANTV, con domicilio en la ciudad de Santiago de Cali, constituida mediante Escritura Pública No. 1712 del 8 de agosto de 1986, de la Notaria Sexta del Círculo de Cali, que en cumplimiento de su objeto social tiene la ejecución de todas las actividades previas, concomitantes y posteriores para producir y emitir televisión regional.

Que en virtud de lo establecido en el artículo 15 de la Constitución Política de Colombia, que consagra la protección a la intimidad personal y el buen nombre, además del derecho que le asiste a las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos y archivos de entidades tanto públicas como privadas; TELEPACIFICO adopta política para la seguridad de la información en el desarrollo de su actividad.

Que de conformidad con el principio constitucional arriba mencionado, así como las demás normas complementarias y las diversas decisiones proferidas por TELEPACIFICO surge la necesidad de adoptar una política institucional de seguridad de la información considerando el papel estratégico de las tecnologías de información y comunicaciones -TIC; además de la importancia de mitigar riesgos alrededor de la información mediante la implementación de planes para el manejo de incidentes, así como las herramientas para respaldar las actividades ejecutadas en TELEPACIFICO, incentivando la cultura de seguridad de información a los usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o pérdidas de información.

Que el fundamento de Política para la Seguridad de la Información de la Sociedad Televisión del Pacifico Ltda. – Telepacífico es buscar la gestión del conocimiento

como base para la mejora continua de la misma, adaptándola a la normatividad vigente en el sector, las tendencias tecnológicas y los cambios en la gestión de procesos y procedimientos tecnológico

Que de acuerdo a lo anterior se resuelve:

**ARTICULO PRIMERO**: **MARCO LEGAL:** la presente resolución esta respaldad por el siguiente marco legal:

- LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- LEY 603 DE 2000: "... el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los programas de software son o no legales"

- LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- LEY 1273 DEL 5 DE ENERO DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- LEY 1341 DEL 30 DE JULIO DE 2009: Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

- DECRETO 2693 DE 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones. DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- LEY 1712 DE 2014; Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.

telepacífico

- DECRETO 2573 DE 2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- LEY ESTATUTARIA 1581 DE 2012: Constituye el marco general de la protección de los datos personales en Colombia.

- DECRETO 1078 DE 2015: Por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de la Información y las Comunicaciones La Política de Tratamiento de Datos Personales ha sido elaborada de conformidad con el Derecho Fundamental de Protección a la Intimidad, establecido en la Constitución Política de Colombia (Artículo 15); en concordancia con los principios generales establecidos en la Ley 1581 de 2012 - por la cual se dictaron disposiciones generales para la protección de datos personales, el Decreto 2952 de 2010, el Decreto 1377 de 2013 y el Decreto 1074 de 2015.

**ARTICULO SEGUNDO:** ADOPTAR el marco institucional de la Política para la Seguridad de la Información de la Sociedad Televisión del Pacifico Ltda. – Telepacífico. Documento que hace parte integral de la presente Resolución.

**ARTICULO TERCERO:** El presente marco de política institucional de seguridad y privacidad de la Política para la Seguridad de la Información podrá ser modificado, adicionado y ajustado previa aprobación del Comité de Gobierno en Línea, de acuerdo al mejoramiento continuo de los procesos y por los requerimientos legales vigentes.

**ARTÍCULO CUARTO**: La presente resolución rige a partir de la fecha de publicación.

Dada en Santiago de Cali, a los veintidós (22) días del mes de marzo de dos mil diez y siete (2017)

**CESAR AUGUSTO GALVIZ MOLINA**
**Gerente**

Elaboro Oficina jurídica LLL
Dirección técnica

Vo.Bo. Jefe Oficina Jurídica
Sociedad Televisión del Pacifico Ltda.
Telepacífico

# SEGURIDAD DE LA INFORMACIÓN

## Política para la Seguridad de la Información de la Sociedad Televisión del Pacifico Ltda. – Telepacífico.


Aprobada por:
**Cesar Augusto Galviz Molina**
Gerente General

Revisión:
**John Carlos Hurtado Gamboa**
Director de Técnica y Sistemas

**Liliana López López**
Jefe de Oficina Jurídica

Proyecto y Elaboró:
**Diana Patricia Delgado Paz**
Coordinadora de sistemas



V01.
Fecha Redacción: Abril de 2017

# TABLA DE CONTENIDO PAG.

# Introducción

La creciente evolución tecnológica que ha logrado TELEPACIFICO a través de la implementación de proyectos de fortalecimiento de la infraestructura TI trae consigo cambios y retos permanentes que requieren ser documentados y controlados de manera simultánea al avance de éstas tecnologías ya que muchas de estas bondades han incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo.

La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger a TELEPACIFICO ante éstas nuevas amenazas.

El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos las empresas, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado, incluyendo a la sociedad civil.

Telepacífico plantea el desarrollo de una política de seguridad que permita identificar el proceder ante el ingreso de personal que tiene acceso a los sistemas de información de la entidad, así como la identificación de los actores y procedimientos a llevar a cabo ante la creación, modificación y eliminación de usuarios, si esta aplica.

Se incluirá también el procedimiento que debe llevarse a cabo para la gestión de usuarios del sistema financiero, sistema de gestión documental, la administración de usuarios de bases de datos y en general el desarrollo de la política de seguridad de la información.

Este documento es desarrollado entre otros con el objetivo de que ***la oficina asesora de Planeación y Desarrollo***, incluya o modifique en el procedimiento OT - PR-05 existente para la gestión Operativa y Tecnológica en el SGC del canal, los roles responsables de la gestión de usuarios de los sistemas informáticos de TELEPACIFICO.

# 2. Recomendaciones generales

## 2.1 CONTRASEÑAS:

Una contraseña se debe considerar al mismo nivel de seguridad que la firma escrita, es decir, es algo *estrictamente personal* y utilizado junto con el nombre de usuario para determinar de forma fehaciente quien realiza una operación, ya que en muchos casos se manejan datos críticos y con un alto grado de confidencialidad. Por ello siempre deben observarse las siguientes directrices:

- Todo usuario debe acceder siempre a un equipo de la red de Telepacífico con el *nombre de usuario que le ha sido asignado*.
- La contraseña es *personal e intransferible*, por lo que *nunca debe cederse o compartirse* a terceras personas ni comunicarse por ningún medio escrito. Lo contrario supondría permitir una suplantación de personalidad, adicionalmente es responsabilidad del usuario que comparte su contraseña, los posibles daños o perdida de la información.
- Las contraseñas no se transmitirán de forma oral cuando exista el riesgo de que terceras personas puedan llegar a conocerlas.
- Cuando un usuario olvide su contraseña se le deberá asignar otra nueva. La asignación de una nueva contraseña solo se hace por medio de comunicación directa del usuario responsable con los operadores de sistemas de Telepacífico.
- La contraseña debe tener una longitud mayor o igual a seis caracteres. No debe coincidir con ninguna palabra o nombre (el de la persona, familiar, aficiones, obtenida de un diccionario, etc.) que pueda permitir que una tercera persona la adivine.
- Las contraseñas deben ser cambiadas periódicamente. La periodicidad del cambio de contraseñas de usuario en Telepacífico es de 60 días.
- El administrador de usuarios informará a sus usuarios de todas estas políticas y velará por su cumplimiento.
- Se debe diferenciar el puesto de trabajo de un usuario de su nombre de usuario y contraseña. Cuando un usuario se traslade de puesto de trabajo, conserva su nombre de usuario y contraseña, aunque trabaje en otro lugar.

## 2.2 CUENTA DE CORREO ELECTRÓNICO:

Los usuarios son los únicos responsables de todas las actividades realizadas con sus cuentas de correo electrónico y su buzón asociado en Telepacífico. En todo momento se deberán cumplir las normas vigentes sobre el Acceso de los Usuarios a los Servicios de Telepacífico y las Leyes Vigentes en Colombia.

- Está prohibido facilitar la cuenta de usuario y buzón a personas no autorizadas.

- Los usuarios deben ser conscientes de la diferencia de utilizar direcciones de correo electrónico suministradas por Telepacífico o privadas ofrecidas por cualquier proveedor en Internet. Las comunicaciones privadas deben realizarse exclusivamente a través de los buzones del proveedor Internet, pero nunca desde las instalaciones Telepacífico y para temas laborales serán usadas en exclusiva las direcciones internas proporcionadas por la entidad.
- Los servicios de correo electrónico suministrados por la Telepacífico pueden ser usados por el personal de Telepacífico de forma incidental para temas personales, excepto si:
  - ✓ interfieren con el rendimiento del propio servicio o suponen un alto coste para Telepacífico.
  - ✓ Interfieren en las labores propias del usuario o de los gestores del servicio de TI.

- Para la difusión de información a grupos de personas existen las ***listas de distribución(grupos en Outlook)***, en cuyo caso deben observarse las siguientes directrices:

  - ✓ En ningún caso se podrán utilizar las listas de distribución para la distribución de información ajena a las finalidades de Telepacífico.
  - ✓ No se deben utilizar las listas de forma indiscriminada, ya que el exceso de información puede llegar a ser tan negativo como su falta.
  - ✓ En los mensajes a las listas se debe evitar incluir archivos binarios como por ejemplo documentos de tamaño elevado (más de 10 Mb) para evitar la degradación del servicio de correo y el llenado involuntario de los buzones de los usuarios.
  - ✓ Serán de obligado cumplimiento las normas y recomendaciones que se elaboren respecto del uso de las listas de distribución.
- Está prohibido realizar cualquiera de los tipos definidos en el Abuso de Correo Electrónico, Además de las siguientes actividades:
  - ✓ Utilizar el correo electrónico para cualquier propósito comercial o financiero ajeno a las funciones propias de Telepacífico.
  - ✓ No se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.
  - ✓ Distribuir de forma masiva grandes cantidades de mensajes sean o no de contenido laboral a direcciones externas a Telepacífico.
- El incumplimiento de la presente normativa supondrá la cancelación inmediata del acceso del usuario sin perjuicio de otras medidas que se puedan emprender en el ámbito laboral o penal.

### 2.3 SOFTWARE:

Los usuarios son los únicos responsables de todas las actividades realizadas a través de las aplicaciones disponibles en las estaciones de trabajo y únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución. Todo software que se encuentre ilegalmente instalado en una estación de trabajo será responsabilidad del y/o los usuarios de dicha estación.

La oficina de sistemas dentro de las labores de mantenimiento de la plataforma TI incluirá la limpieza de las estaciones de trabajo a nivel de software ilegalmente instalado al menos 2 veces en el año.

# 3. Política de Seguridad de la Información

La información es un recurso que, como el resto de los activos, tiene valor para Telepacífico y por consiguiente debe ser debidamente protegido, clasificado y valorado.

Telepacífico define su política de seguridad de la información de acuerdo a la normatividad legal vigente identificada a continuación:

- **LEY 23 DE 1982:** "Sobre Derechos de Autor".
- **CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991**; Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".
- **LEY 527 DE 1999;** por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **LEY 603 DE 2000: "…** el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los programas de software son o no legales".
- **LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **LEY 1273 DEL 5 DE ENERO DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **LEY 1341 DEL 30 DE JULIO DE 2009:** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **DECRETO 2693 DE 2012** Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones. DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **LEY 1712 DE 2014;** Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.
- **DECRETO 2573 DE 2014** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- **LEY ESTATUTARIA 1581 DE 2012:** Constituye el marco general de la protección de los datos personales en Colombia.
- **DECRETO 1078 DE 2015:** Por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

De acuerdo con la información estipulada se definen los siguientes elementos principales de la política de seguridad de la información de Telepacífico y se establece que todos los funcionarios que tengan acceso a los sistemas de información de la entidad, deben cumplir con toda la reglamentación mencionada.

Nuestra política de seguridad se centra en los elementos funcionales del sistema de Información que pueden resultar vulnerables como son:

- El Centro de Cómputo.
- La red de área Local - LAN.
- El uso de internet.
- El correo electrónico corporativo.
- Las bases de datos.
- Las aplicaciones.
- El sistema de virtualización - VmWare.

- El sistema de respaldo - Backup".
- Los sistemas de almacenamientos - data storage.
- El Directorio activo.

### 3.1 Responsabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del TELEPACÍFICO y la ciudadanía en general.

Es responsabilidad de **la *Dirección de Técnica y Sistemas*** establecer la Política de Seguridad de la Información como parte de sus herramientas gestión y es responsable de definir los estándares, procedimientos y lineamientos que garanticen su cumplimiento.

***El área de Recursos Humanos*** es responsable de dar a conocer la política de Seguridad de Información a todos los nuevos colaboradores que inicien un vínculo laboral con Telepacífico y tengan acceso a información de la entidad.

Es responsabilidad de la ***Oficina Asesora de Planeación*** formalizar este documento dentro del sistema de Gestión de Calidad de Telepacífico y socializarlo periódicamente. Adicionalmente debe realizar las modificaciones que correspondan en el procedimiento OT - PR-05 existente para la gestión Operativa y Tecnológica que apliquen según la reglamentación y nuevos procesos que no se encuentren documentados en dicho procedimiento.

Es responsabilidad de la ***Oficina Jurídica*** aplicar las penalidades que correspondan en caso de incumplimientos de la política de Seguridad de Información por parte de los funcionarios de Telepacífico

***Todos los funcionarios y/o contratistas*** serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

### 3.2 Cumplimiento

Todas las personas cubiertas por la responsabilidad deberán dar cumplimiento un 100% de la política.

El cumplimiento de la Política de Seguridad de la Información es de carácter obligatorio. Si los colaboradores, contratistas y/o terceras partes violan estas

políticas, Telepacífico se reserva el derecho de tomar las medidas correspondientes, de acuerdo con las sanciones establecidas por la Oficina Asesora Jurídica.

Si existieren excepciones al cumplimiento de la Política de Seguridad de la Información, dichas excepciones deben ser aprobadas por la Dirección de Técnica y Sistemas, la cual puede requerir autorización de la Gerencia de Telepacífico. Todas las excepciones a la Política deben ser formalmente documentadas, registradas y revisadas

## 3.3 Objetivos

Principalmente el establecimiento de este documento tiene como objeto garantizar la continuidad de los servicios, proteger los recursos y los componentes de infraestructura y asegurar el eficiente cumplimiento de los objetivos de negocio y los requisitos de seguridad destinados a impedir infracciones o violaciones de seguridad de la información en Telepacífico. Según lo anterior se establecen los siguientes objetivos específicos:

- Establecer un procedimiento o proceso documentado para la gestión de los usuarios que hacen uso del aplicativo financiero APOTEOSYS.
- Establecer un procedimiento o proceso documentado para la gestión de los usuarios que hacen uso del sistema de Gestión Documental – SADE.
- Establecer un procedimiento o proceso documentado para la gestión y administración de los usuarios que hacen parte del dominio de la red de datos de Telepacífico.
- Documentar el procedimiento de Reporte e investigación de incidentes de seguridad de la información y los responsables del mismo.
- Establecer las directivas que Telepacífico emplea o debe emplear para la protección contra software malicioso y hacking.
- Documentar el proceso de Copias de Seguridad.
- Programar periódicamente capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad para el personal encargado de la administración de TI.
- Documentar los procedimientos correspondientes a la gestión de seguridad la de Red LAN y el acceso a internet.
- Reglamentar el intercambio de Información con Organizaciones Externas.
- Regular el uso del Correo Electrónico.
- Establecer las directrices para la Instalación de Software.

- Establecer las normativas y lineamientos para el uso de Medios de almacenamiento temporal.
- Administración y uso del servidor de Archivos.
- Documentar la prestación del servicio de Soporte técnico.

# 4. Identificación de activos de información

El Decreto 103 de 2015 define el Registro de Activos de Información como "el inventario de la información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal". En este sentido, la identificación de Activos de Información se centraría sólo en los activos de información de tipo datos o información.

Adicionalmente, el mencionado decreto establece en su Artículo 38 - Componentes del Registro de Activos de Información, que dicho registro debe contener, como mínimo, los siguientes componentes:

1. Todas las categorías de información del sujeto obligado.
2. Todo registro publicado.
3. Todo registro disponible para ser solicitado por el público

En relación con el numeral 1, el Parágrafo 1 del artículo 38 de la mencionada norma, establece que una categoría de información es "toda información de contenido o estructura homogénea, sea física o electrónica, emanada de un mismo sujeto obligado como resultado del ejercicio de sus funciones y que pueda agruparse a partir de categorías, tipos o clases según sus características internas (contenido) o externas (formato o estructura).

Los activos fijos que hacen parte de la estructura informática de Telepacífico son los siguientes:

- Base de datos del sistema financiero.
- Base de datos del sistema de gestión documental
- Archivo físico.
- Archivo Digital.
- Backup de los servidores de TI.

A continuación se describe cada uno de los activos identificados:

***Base de datos del sistema Financiero:*** Corresponde a los archivos que contienen la estructura de las tablas y la información contenida en ellas, pertenecientes a la base de datos en formato Oracle, la cual soporta el sistema financiero de Telepacífico llamado APOTEOSYS.

***Base de datos del sistema de gestión documental:*** Corresponde a los archivos que soportan el sistema de gestión documental SADE, utilizado para la gestión de documentos en Telepacífico.

***Archivo Físico***: Telepacífico toma la definición de su archivo físico, la dictada por la Ley General de Archivos establecida en la LEY 594 DE 2000, la cual define el ***archivo*** como el "Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia". El archivo Físico de Telepacífico se almacena según las tablas de retención documental establecidas para tal objeto.

***Archivo Digital***: en Telepacífico se cuenta con varios medios de almacenamiento de archivo digital los cuales corresponden a:

- **Sistema de gestión documental SADE**: contiene la información de documentos digitalizados a en la ventanilla única y tu trámite a través de las divisiones de la entidad.
- **El servidor de archivos de TI:** Corresponde a la información que es utilizada diariamente por el personal de la entidad para el desempeño de sus funciones

***Backup de los Servidores de TI:*** Corresponde a la copia de seguridad de los archivos almacenados en los medios magnéticos dispuestos por la división Tecnica y sistemas para tal función, los cuales contienen la configuración y copia de la información que es utilizada diariamente por el personal de la entidad para el desempeño de sus funciones, adicionalmente contiene los archivos de configuración que permiten reestablecer los servicios de TI en caso de presentarse perdida o daño parcial y/o total de la información en los servidores.

### 4.1 Control de acceso a los Activos de Información

Para la consulta de documentos cargados en el ***software de Gestión Documental SADE***, se establecerán perfiles de acceso a los funcionarios y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán

establecidos por el Jefe o Director de la Division, quien comunicará al Líder de gestión documental el listado con los funcionarios y sus privilegios.

El acceso a los documentos digitales del ***servidor de archivos de TI*** estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Jefes de Division u oficina.

## 5. Seguridad de la información en el Recurso Humano

El control de seguridad y acceso a la información de la plataforma TI de la entidad se hace a través del acceso a los recursos de red establecido en el directorio activo, el cual almacena información de una organización en una base de datos central, organizada y accesible.

Para permitir los accesos a los recursos TI cada funcionario debe tener un usuario protegido con contraseña, el cual se crea por el personal de TI previa autorización de la oficina de recursos humanos y del jefe de la división a la cual pertenece el nuevo funcionario.

Al finalizar su tiempo en la organización los usuarios creados en directorio son deshabilitados por parte del personal de TI, conservando políticas de seguridad e información personal por un periodo de máximo un año, en caso de que el funcionario tenga nuevamente un vínculo contractual con Telepacífico. Este procedimiento solo se lleva a cabo cuando la oficina de recursos humanos lo solicita.

## 6. Seguridad Física y del Entorno

El control de seguridad del entorno que se relaciona con la infraestructura TI de Telepacífico debe permanecer bajo un protocolo de seguridad que impida que los equipos sean manipulados por personal no apto para dichas labores, para tal fin Telepacífico cuenta con sistemas de control de acceso automatizado en la puerta del centro de datos, en el cual se encuentra instalado el hardware que soporta la plataforma TI.

El centro de datos de Telepacífico debe permanecer en condiciones físicas que cumplan con las recomendaciones referentes a Instalaciones eléctricas, Aire acondicionado y Seguridad establecidas en la norma "ICREA-Std-131-2015" y diligenciar mensualmente el formato de verificación del centro de cómputo:

| No. ACT. | ACTIVIDAD | RESPONSABLE (Cargo) |
|---|---|---|
| 1 | Revisar temperatura del centro de cómputo, esta debe estar siempre en 70 grados en el control de la temperatura. | Coordinador de sistemas |
| 2 | Verificar que los equipos de cómputo (servidores), permanezcan bajo llave y con sesiones cerradas. | Coordinador de sistemas |
| 3 | Verificar que la puerta de acceso permanezca cerrada. | Coordinador de sistemas |
| 4 | Verificar que el control del aire acondicionado permanezca encendido. | Coordinador de sistemas |
| 5 | Verificar que las conexiones eléctricas de los servidores se encuentran encendidas y en buen estado. | Coordinador de sistemas |
| 6 | Verificar fecha de vencimiento de extintores. | Coordinador de sistemas |
| 7 | Verificar que dentro del centro de cómputo no exista material que represente riesgos de incendio (Cajas, Papel, madera) | Coordinador de sistemas |
| 8 | Verificar que el switch de red donde se encuentran conectados los servidores esté funcionando correctamente. | Coordinador de sistemas |
| 9 | Consignar en la bitácora de revisión física la verificación realizada de acuerdo a los puntos anteriormente nombrados en el documento revisionFisicaCentroComputo.xls | Coordinador de sistemas |

Se deben ofrecer las mejores condiciones del entorno en las locaciones donde se encuentran instalados los equipos de cómputo y dispositivos de entrada y salida de información, se deben cumplir las siguientes especificaciones:

- Los equipos y dispositivos deben de estar en un lugar fresco y con el mueble ideal para estos.
- La corriente eléctrica debe de ser confiable y estable.
- No debe de encontrarse junto a objetos que puedan caer sobre ella tales como ventanas, mesas, sillas, lámparas, etc.
- La CPU no debe de estar en el piso, debe ubicarse en el mueble donde se tiene el resto del equipo.
- Cada equipo y/o dispositivo debe de estar conectado a una toma de energía regulada.
- El equipo y/o dispositivo debe apagarse de manera correcta, no desconectarse de la energía estando encendido.
- El equipo y/o dispositivo debe estar cubierto por fundas especiales para que no penetre el polvo, dichas fundas deben ponerse cada que se apaga.
- Limpiar regularmente el teclado, el ratón y el mouse pad, para liberar de polvo el espacio de desplazamiento.
- No debe de desconectarse ningún dispositivo o parte interna si no ha sido apagado la CPU.
- No deben consumirse alimentos o bebidas encima del equipo y/o dispositivo.

# 7. Administración Segura de la Plataforma TI

La administración de la plataforma TI se encuentra en el marco del proceso de Gestión Operativa y Tecnológica de Telepacífico, dicho proceso contempla los siguientes aspectos de seguridad:

### 7.1 Sistema de gestión documental – SADE

Telepacífico cuenta con el licenciamiento de una aplicación web llamada SADE, desarrollada por la empresa Sysdatec S.A.S. la cual permitió automatizar el proceso de gestión documental dentro de la entidad. Dicho sistema cuenta con un control de acceso a través de usuarios administrados por el líder del proceso de gestión documental de la entidad. Las políticas de manejo de los usuarios para el sistema SADE son las siguientes:

- Las credenciales de acceso a usuarios operativos son asignadas por el usuario administrador, el cual corresponde al líder del proceso de gestión documental previa autorización del director de la Division Administrativa.
- Ejecución de Backup diario de la base de datos del sistema.
- Proceso de restauración del archivo de base de datos a una base de datos de prueba cuatro (4) veces al año alternando desde medios de almacenamiento físicos y lógicos.
-

### 7.2 Sistema Financiero – APOTEOSYS

En Telepacífico se cuenta con una licencia de uso a término indefinido del sistema APOTEOSYS, el cual es una solución de software que integra los módulos de CONTABILIDAD, TESORERIA, PRESUPUESTO PUBLICO, ACTIVOS FIJOS, FACTURACION DE SERVICIOS, COMPRAS e INVENTARIOS. Este sistema fue desarrollado y es actualizado por la firma HEINSOHN TECHNOLOGY, como una herramienta de soporte lógico de las operaciones de gestión administrativa y financiera.

Las políticas de manejo de los usuarios para el sistema APOTEOSYS son las siguientes:

- Ejecución de Backup diario de la base de datos del sistema.
- Proceso de restauración del archivo de base de datos a una base de datos de prueba cuatro (4) veces al año alternando desde medios de almacenamiento físicos y lógicos.

### 7.3 Gestión de usuarios de Dominio

Para la gestión de usuarios en el directorio activo y los vinculados al dominio REDTELEPA, los cuales tienen permiso de acceso a las unidades de red y sistemas de la entidad, se debe llevar a cabo las siguientes labores:

***Creación de usuarios***: La oficina de Recursos humanos de Telepacífico debe llevar a cabo una solicitud formal vía correo electrónico dirigida a la oficina de sistemas, solicitando la creación de un usuario nuevo de dominio, indicando para cada uno su nombre completo, el cargo que ocupara en la entidad, el número de cedula y la división a la que pertenece. Teniendo en cuenta que la entidad tiene unidades de red con información específica de diferentes proyectos, se debe indicar en la misma solicitud si el nuevo usuario requiere acceso especial a alguna de las unidades

mencionadas; especificando si los permisos requeridos debes ser de escritura, lectura, ejecución, etc.

***Modificación de usuarios***: Para llevar a cabo la modificación de características de un usuario, se debe hacer la solicitud pertinente vía correo electrónico especificando detalladamente el requerimiento y estar disponible para responder a las consultas realizadas por el personal de sistemas, con objeto de aclarar la solicitud. Los usuarios de dominio se pueden crear, habilitar y deshabilitar más no eliminar.

***Habilitación/Deshabilitación de usuarios***: La oficina de recursos humanos debe indicar a través de comunicación formal vía correo electrónico cuando un usuario debe ser habilitado o deshabilitado según los movimientos del personal.

### 7.4 Seguridad de Red de datos

En Telepacífico se cuenta con una red LAN para la comunicación e interconexión entre los dispositivos TI, la cual está distribuida de manera que permita eficiencia y eficacia en la transmisión de información, cuenta con especificaciones de seguridad que permiten salvaguardar la estabilidad en las comunicaciones. A nivel de infraestructura, se encuentra soportada por switches con tecnología PoE, que soportan velocidad de transmisión de hasta 1GB/s y funcionan en la capa 3 del modelo OSI, se cuenta con cableado de red en categoría 6A.

Telepacífico cuenta con la solución UTM (Seguridad Perimetral de la red) Fortinet en su versión 100D, la cual Combina Firewall, IPSec, SSL VPN, control de aplicaciones, prevención de intrusiones, antivirus, antimalware, antispam, seguridad P2P, y filtrado Web en un sólo dispositivo. Se debe contar con un contrato actualizado para tener el acceso a la descarga de las actualizaciones de la solución. Así mismo velar por el cumplimiento de políticas de control en el dispositivo que impidan acceso a sitios web no autorizados, sitios de descarga masiva, páginas web fraudulentas, etc.

El servicio de Internet es una herramienta de trabajo para los usuarios de Telepacífico, que lo requieran como apoyo a sus funciones. Anualmente se establece un contrato con empresas proveedoras de servicios de telecomunicaciones, las cuales prestan el servicio de internet banda ancha a Telepacífico, el que a su vez es distribuido desde el sistema de seguridad perimetral Implementado para establecer controles de:

***Reglamentación:***

- Todo usuario que requiera acceso a internet desde las instalaciones de Telepacífico, deberá ser autorizado individualmente por el personal de Sistemas de la entidad.
- Telepacífico se reserva el derecho de restringir el acceso de los usuarios a ciertos sitios web, así como también la restricción parcial o total de acceso a internet de los mismos, a través del personal de la oficina de sistemas.
- Toda la información entrante o saliente a internet puede ser monitoreada y/o registrada sin previo aviso.
- Se disponen estándares y cuotas de navegación, en relación al tráfico, contenidos, entre otros, los cuales serán monitoreados y escalados a los directores de cada división, según la situación así lo requiera.
- La ley colombiana contenida en las normas mencionadas y complementadas con el Convenio de Berna, Los tratados Internet WCT y WPPT de 1996 y el Acuerdo de los ADPIC en la Organización Mundial de Comercio, es clara al determinar que el autor o el titular de los derechos de explotación tiene el derecho exclusivo de autorizar o prohibir la reproducción de su obra; la comunicación pública, la transformación y la distribución de ejemplares, por cualquier medio conocido o por conocer. Esto significa en el derecho normativo latinoamericano, que cualquier forma de explotación que de una obra se pueda realizar, se convierte en derecho exclusivo en cabeza del titular así dicha forma de explotación no esté expresamente contemplada en la ley. Por ello, en general, y salvo casos de excepciones muy específicos, la descarga de contenidos protegidos por el derecho de autor o conexos como libros, música, películas, obras fotográficas, entre otras, requiere de previa y expresa autorización del titular.
- Está prohibido divulgar información interna de Telepacífico en redes sociales, blogs, sitios web u otros medios de comunicación electrónica sin la debida autorización del comité de Gobierno en Línea, a través de su representante y/o el representante legal de la entidad.

### 7.5 Control de acceso al centro de cómputo

Telepacífico cuenta con un sistema de control de acceso físico que permite regular el ingreso de personal al área de data center, solo el personal que tenga roles de administración de alguna de las plataformas cuyo hardware se encuentra instalado en

este espacio, puede tener acceso presencial al centro de cómputo. Adicionalmente se debe llenar la bitácora de registro del ingreso del personal indicando brevemente la razón o causa del ingreso. El formato correspondiente a la bitácora es el "OT-FO-07 Acceso Centro Computo - Rev. 01" registrado en el SGC de Telepacífico.

### 7.6 Protección contra software malicioso y Hacking

Telepacífico cuenta con licenciamiento anual del servicio antivirus a través del software Kaspersky desarrollado por Kaspersky Lab., el cual ofrece protección a las estaciones de trabajo y servidores contra software malicioso

### 7.7 Copias de seguridad

Telepacífico cuenta con una solución de software y hardware para la ejecución de copias de seguridad de la información más relevante de la entidad y la cual conforma los medios magnéticos de contingencia para recuperación en caso de presentarse algún desastre informático. Dicha solución está conformada por los siguientes ítems:

- Software para gestión de copias de seguridad HP Dataprotector.
- Data storage con Tb de capacidad de almacenamiento
- Dispositivo de lecto-escritura LTO para copias de seguridad físicas en Tapes.
- 19 LTO tapes de 400 GB a 800 GB para backup diario
- 6 LTO tapes de 800GB a 1.6 TB de capacidad Para backup semanal.
- 12 LTO tapes de 800 GB a 1.6 TB de capacidad para backup mensual.
- Se cuenta con un Tape LTO para backup Anual el cual se reemplaza en enero de cada año y se deja en custodia de una empresa externa de seguridad hasta el 31 de diciembre del siguiente año.

El procedimiento para la ejecución de los backup se encuentra en el documento anexo "Disposiciones y Procedimientos Backup Telepacífico".

### 7.8 Directrices de Instalación de Software

Dentro del directorio activo se llevó a cabo la configuración de políticas de seguridad que impiden que los usuarios sin privilegio de administrador puedan instalar software en los equipos de cómputo que se encuentran unidos al dominio REDTELEPA.COM. Adicionalmente se contemplan las siguientes reglas:

- Solo se pueden utilizar los browser instalados en los equipos de cómputo por el personal de sistemas de la entidad.

- No se puede instalar software sin licenciamiento adscrito a Telepacífico.
- No se puede instalar en equipos de la entidad software con licenciamiento de terceros.
- No se puede instalar en los equipos de la entidad software sin licenciamiento o por fuera del tiempo de licenciamiento Trial, con llaves o software ilegal.
- No está permitido instalar licencias propiedad de Telepacífico en computadores personales o de terceros.
- No está permitido desinstalar software de los equipos de cómputo de Telepacífico.

### 7.9 Almacenamiento servidor de archivos

Telepacífico cuenta con un servidor para almacenamiento de archivos asociados a las labores de los usuarios pertinentes a las funciones definidas para cada uno. Se debe tener en cuenta las siguientes directrices en cuanto a las unidades de red del servidor asignadas a los usuarios:

- La unidad (F:) corresponde al espacio donde cada usuario debe grabar su información personal correspondiente a su gestión laboral. Esta unidad no se configura para Directores de Programas, Productores, Realizadores y practicantes quienes pueden almacenar su información personal en los equipos asignados.
- En la unidad (G:) pueden grabar los archivos que sean de uso común en cada división, pues a ella solo tienen acceso los usuarios que estén dentro de cada grupo de trabajo. Los grupos de trabajo están organizados por Divisiones, Oficinas y cada uno de los programas de Telepacífico.
- La unidad (K:) es una unidad común para todos los usuarios de la red de Telepacífico, esta se debe utilizar para el intercambio de archivos entre los diferentes grupos de trabajo, después de usar los archivos se deben de eliminar. *Este directorio no posee respaldo.*
- No está permitido almacenar de manera permanente en estas unidades de red archivos de imagen, audio y/o video.
- A las unidades de red especiales (diferentes a las ya mencionadas), se les aplicara las reglas específicas solicitadas y concertadas con el usuario solicitante al momento de su creación.

### 7.10 Control de Claves y Nombres de Usuario

En Telepacífico se manejan diferentes reglas para la creación de usuarios y contraseñas:

1. **Directorio activo o usuarios de red:** Para la creación de los nombres de usuarios de red se debe tener en cuenta el cargo del usuario, la división a la que pertenece y la cantidad de usuarios con el mismo perfil, de tal manera que se puedan incluir estos tres aspectos en el nombre de usuario, por ejemplo:

   **Datos del Funcionario:** Maria Paola Rengifo, *Asistente* número *3* de *producción*, cedula 1.158.746.288

   **Nombre de usuario:** asisprod3.

   **Contraseña:** La contraseña de usuario asignada inicialmente es <<'mr1158746288'>> y corresponde a la primera letra de su nombre, la primera de su apellido y su número de cédula, todo seguido y sin espacios.
2. **Usuarios del sistema financiero:** Para la creación de usuarios del sistema financiero o ERP Apoteosys, se debe tener en cuenta el cargo del funcionario a quien se asigna, del cual se crea una abreviatura para la asignación del nombre de usuario.

### 7.11 Soporte Remoto

Telepacífico dentro del marco de la implementación de la estrategia de teletrabajo ha concertado la adquisición de una software de licenciamiento perpetuo de un software para gestión de soporte remoto llamado Team Viewer, esto con el fin principal de mejorar a nivel de eficacia y eficiencia la prestación de servicios de soporte a los usuarios de la entidad así como facilitar a los proveedores de servicios de soporte el acceso remoto a los terminales y servidores de la entidad.

La información del licenciamiento de dicha plataforma se encuentra en el inventario de licencias de software el cual reposa en el archivo digital de Telepacífico, en el área de Tecnica y sistemas.

# 8. Adquisición, Desarrollo y Mantenimiento de Sistemas Software

Actualmente en Telepacífico no se encuentra definida una política para llevar a cabo desarrollo de software específico para las funciones automatizadas de la entidad, sin embargo cuando se hace necesaria una solución de software, se lleva a cabo un proceso de contratación de un tercero que proporcione dicha solución; el proceso de contratación se encuentra registrado en el *Manual de contratación de Telepacífico, en la Resolución 259 de 2016* "Por medio de la cual se deroga la Resolución No. 196 del 28 de julio 27 de 2014 y se expide el nuevo manual de contratación de la sociedad de televisión del pacífico Ltda. – Telepacífico".

Así mismo cuando se requiere llevar a cabo la contratación de mantenimiento, renovación de licenciamiento o soporte técnico, se procede a realizar un estudio previo a la contratación y se continúa el proceso con las especificaciones consignadas en el manual de contratación.

# 9. Mantenimiento de la Infraestructura TI

Para llevar a cabo el mantenimiento tanto correctivo como preventivo de la plataforma TI de Telepacífico, se desarrolla un cronograma durante el mes de enero de cada año, en el cual se contempla la ejecución de las siguientes labores:

**Mantenimiento Preventivo CPU**: Retiro de la suciedad acumulada en las tarjetas, disco duro y en la fuente de poder, limpieza de contactos en tarjetas y memoria RAM, retiro de disipador del procesador y aplicación pasta térmica refrigerante, limpieza de todas las partes internas de la CPU con limpiador electrónico, ensamble y ajuste total de la CPU, limpieza general externa con producto limpiador antiestático y silicona seca. Identificación de componentes internos (condensadores, RAM, ventiladores, etc) en mal estado y registro de los mismos en la Hoja de Vida de cada equipo. Actualización de información del equipo en la Hoja de vida y Registro de las actividades realizadas.

**Mantenimiento Preventivo Monitor**: eliminación de polvo externo y residuos presentes con soplador, limpieza general externa con producto limpiador antiestático y silicona seca, se realizan ajustes y calibración de video.

**Mantenimiento Preventivo Teclado y mouse**: eliminación del polvo externo e interno y residuos con soplador, calibración de sensores si es necesario, limpieza general externa con producto antiestático y silicona seca.

**Mantenimiento Preventivo Escáner e Impresora:** eliminación de polvo externo e interno y los residuos presentes con soplador, retiro y limpieza de bandejas, retiro de tóner o cartucho, lubricación de piñones y arrastre de papel, calibración y ajustes en general. Llenado de documento de diagnóstico de deterioro de piezas y consumibles, indicando específicamente que partes se deben reemplazar para el correcto funcionamiento del dispositivo. (Se adjunta hoja de formato).

Dado que los equipos adquiridos por Telepacífico se solicitan siempre con al menos 3 años de garantía por parte del fabricante, al presentarte una falla o se detecte necesidad de mantenimiento o mejora, el paso inicial es proceder con la ejecución de dicha garantía.

En caso de que los dispositivos o equipos de cómputo se encuentren fuera de garantía se lleva a cabo la siguiente evaluación:

- **Impresoras, escáneres, fotocopiadoras y faxes**: Se realiza dos veces en el año, si el personal de la oficina de sistemas cuenta con el conocimiento suficiente para llevar a cabo un mantenimiento correctivo y evaluativo de estos dispositivos. En caso de que el personal de sistemas no cuente con los conocimientos certificados para el desarrollo de esta actividad se procede a la contratación de un tercero que cuente con experiencia y certificación en la labor de mantenimiento preventivo y correctivo de los dispositivos.

- **Computadores de escritorio y portátiles**: Se realizan mantenimientos de software de manera periódica durante todo el año, aproximadamente 2 al año por parte del personal de sistemas. El mantenimiento de hardware se realiza dos veces en el año, si el personal de la oficina de sistemas cuenta con el conocimiento suficiente para llevar a cabo un mantenimiento correctivo y evaluativo de estos dispositivos. En caso de que el personal de sistemas no cuente con los conocimientos certificados para el desarrollo de esta actividad se procede a la contratación de un tercero si los equipos se encuentran fuera de garantía.

# 10. Reporte e investigación de incidentes de Seguridad Informática.

**Reporte de incidentes de seguridad de información:** La oficina de sistemas es responsable de reportar los eventos que afecten la integridad de los activos de información de la entidad, dicho reporte se debe hacer de manera formal a través de una circular informativa dirigida al director de la Division de Tecnica y sistemas.

**Investigación de incidentes de seguridad de información**: La oficina de sistemas es responsable de reportar los eventos que afecten la integridad de los activos de información de la entidad, dicho reporte se debe hacer de manera formal a través de una circular informativa dirigida al director de la División de Técnica y sistemas, de acuerdo al procedimiento que se establezca para este hallazgo.

Una vez se establezca la veracidad, pruebas e impacto del incidente, se enviará el informe a la oficina asesora jurídica para su respectivo proceso disciplinario.

# Referencias


- POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN – ICETEX http://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Politica_seguridad_informacion.pdf

- Elaboración de la política general de seguridad y privacidad de la información – MINTIC. https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

- Manual de contratación de Telepacífico – RESOLUCION 259 DE 2016.

- Disposiciones y Procedimientos Backup TP – Oficina de Sistemas.

# Términos y Definiciones

- **Ataques cibernéticos o informáticos**: Un ataque informático es un intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red.
- **ciberdefensa y ciberseguridad**: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.
- **Data Storage**: espacio física de almacenamiento de datos.
- **Backup**: El backup es una palabra que en ámbito de la tecnología y de la información, se refiere a una copia de seguridad o el proceso de copia de seguridad, específicamente del archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.
- **Switch**: también llamado conmutador, es un dispositivo de interconexión de redes informáticas. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro.
- **Tecnología PoE**: La alimentación a través de Ethernet (Power over Ethernet, PoE) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE.
- **UTM**: (en inglés: Unified Threat Management) o gestión unificada de amenazas, es un término de seguridad de la información que se refiere a una sola solución de seguridad, y por lo general un único producto de seguridad, que ofrece varias funciones de seguridad en un solo punto en la red.
- **Antimalware:** es un tipo de programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas TI. Los términos antivirus y antimalware se utilizan a menudo como sinónimos ya que los virus informáticos son un tipo específico de malware
- **Antispam:** Aplicación o herramienta informática que se encarga de detectar y eliminar el correo basura