CONTENIDO

1. INTRODUCCIÓN

TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO determina la información como un activo de alta importancia para la entidad porque permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información. En el presente manual se establecen las políticas que integran todo en materia de seguridad de la información, las cuales deben ser adoptadas por los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO ; estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001:2013 y al modelo de seguridad y privacidad de la información de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. La seguridad de la información es para TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, una labor prioritaria que exhorta a todos a velar por el cumplimiento de las políticas establecidas en el presente manual.

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

2. OBJETIVO

Establecer las políticas que regulan la seguridad de la información en TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, bajo el liderazgo del Área de Técnica.

3. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el Comité de Gestión y Desempeño Institucional.

Estas políticas como parte de Seguridad de la Información, tiene alcance en todos los procesos que hacen parte TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, verificándolo y aplicándolo.

4. TÉRMINOS Y DEFINICIONES

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Activo: Según [ISO IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO Se pueden clasificar de la siguiente manera:

- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el DAPRE. Ejemplo: archivo de Word “listado de personal.docx”.
- **Personal:** Es todo el personal de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, el personal subcontratado, los clientes, usuarios y en

general, todos aquellos que tengan acceso de una manera u otra a los activos de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO. Ejemplo: Pepito Pérez.

- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.
- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: equipo de cómputo, teléfonos, impresoras.
- **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina Financiera.
- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

o Detectar cualquier alteración en los servicios TI.
o Registrar y clasificar estas alteraciones.
o Asignar el personal encargado de restaurar el servicio.

Alcance: Ámbito de la organización que queda sometido todo lo relacionado con Seguridad de la Información. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Cifrar: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiere proteger.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora de la SI - **Seguridad de la Información**.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: Según [ISO IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evento: Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

FTP: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Gusano (Worm): Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO IEC TR 18044:2004]: 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.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.), que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Tratamiento de riesgos: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1 POLITICA DE USO DE CORREO ELECTRÓNICO

RESUMEN: Esta política establece la responsabilidad y lineamientos mínimos que deben cumplir todos los usuarios de correo electrónico institucional asegurando el uso correcto del mismo como herramienta de trabajo de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

INTRODUCCIÓN: TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO ofrece a sus colaboradores el servicio de intercambio de mensajes a través de una cuenta de correo electrónico con dominio propio de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO utilizando la plataforma de ***Gmail***. Para facilitar el desarrollo de sus funciones, por lo tanto, los usuarios del correo electrónico son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO se compromete a entregar un correo electrónico a sus empleados siguiendo lo estipulado en la política de correo electrónico, buscando de esta manera garantizar el uso adecuado de todos los sistemas contando con estrategias y medidas de seguridad de la información.

ALCANCE: Esta política aplica a los funcionarios, contratistas y terceros relacionados con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO que cuenten con una cuenta de correo corporativo de la entidad.

OBJETIVO: Establecer las responsabilidades y lineamientos mínimos que deben cumplir todos los empleados, contratistas y terceros que haga uso del correo institucional con el fin de garantizar la correcta función del mismo, asegurando un mejor aprovechamiento de esta herramienta de trabajo que provee TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIOS:

- El correo institucional es un medio formal y oficial de comunicación de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO siendo una herramienta de trabajo que facilita las funciones propias de los empleados y contratistas.
- El desarrollo de esta política es con el fin de fomentar responsabilidad, respeto, integridad y seguridad de la información.
- TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO se reserva el derecho de deshabilitar, modificar o eliminar la cuenta de correo electrónico institucional en las cuales se evidencie el uso inadecuado o incurran en el incumplimiento de las políticas plasmadas en este documento o el negocio lo requiera.
- Para los usuarios pertenecientes a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO de correo electrónico se identificará de la siguiente manera: nombre de la cuenta según (rol área) seguido del: @dominio. El nombre para mostrar será equivalente al cargo o actividad a desempeñar; cualquier excepción al nombre debe ser aprobado con anterioridad por el personal encargado en TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Los usuarios de los correos institucionales deben tener la responsabilidad de la clasificación de los correos spam.
  - Emplear la opción de copia oculta (CCO) cuando se envía un mensaje de tipo informativo a más de una persona destinataria.
  - Responder solamente al emisor del correo en caso de que se haya solicitado confirmación de recibido.

- Revisar las direcciones de los destinatarios antes de enviar el mensaje.
- Valorar la utilización de la opción de copia oculta para enviar un correo electrónico a múltiples destinatarios.
- Con objeto de no difundir injustificadamente direcciones de correo de terceros al reenviar un correo electrónico, valorar la opción de eliminar las direcciones de los destinatarios anteriores.
- Identificar de forma clara y concisa el asunto.
- No incluir datos personales en el asunto.
- Evitar palabras o expresiones que puedan activar los programas antispam.
- Revisar el contenido del mensaje, los archivos adjuntos y su destinario antes de enviarlo.
- Emplear el pie de firma automático de los mensajes de correo electrónico, basados en el modelo establecido, que incluye la cláusula de confidencialidad. En caso de que el correo sea compartido identificar el nombre del emisor.
- Cuando se trate de mensajes con fines personales no se deberá utilizar el correo institucional.
- Evitar enviar archivos excesivamente grandes.

- Las claves de acceso a los correos electrónicos deben cumplir con la política de gestión de claves de acceso a los sistemas de información para asegurar un alto nivel de protección a la información.

- Los usuarios de los correos electrónicos se deben hacer responsables de la información que manejan y envíen mediante dicho correo, en caso de que el usuario borre de forma accidental algún correo o carpeta de su cuenta de correo corporativa de Televisión Regional del Oriente.

- Los correos institucionales se emplearán única y exclusivamente para una finalidad operativa y administrativa y deben seguir los siguientes lineamientos:

  - Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura tecnológica de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO se consideran bajo el control de la entidad. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, y no debe utilizarse para ningún otro fin.
  - Los usuarios del servicio de correo electrónico no deben realizar el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad o terceros.
  - El servicio de correo electrónico no debe utilizarse para el envío de cadenas de mensajes.
  - El servicio de correo electrónico de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO no debe usarse para el envío de mensajes masivos y, en casos excepcionales, se debe utilizar la opción de copia oculta para todos los destinatarios.

- El servicio de correo electrónico de la entidad no debe ser utilizado para el envío de mensajes de gran tamaño que pueden congestionar la red; para ello deben emplearse otros medios como, por ejemplo, los servicios de la nube de archivos digitales ***(Google Drive, WeTransfer, ydray)*** o en su defecto medios extraíbles como discos externos o memorias USB o mediante empresas de correspondencia certificada.
- A los usuarios del servicio de correo electrónico que se desvinculen de la entidad, se les bloqueará la cuenta de correo y esta misma será reemplazada en caso que no haya cuentas disponibles o se necesite un nuevo correo electrónico, previa orden y autorización por parte de Gerencia o Talento Humano.
- A los usuarios de correos misionales o estratégicos en dado caso que se desvinculen de la entidad se les bloqueará la cuenta de correo electrónico y se habilitará nuevamente hasta que sea reasignada al nuevo líder o encargado designado por gerencia.
- La apariencia de la firma de correo electrónico está establecida con los parámetros de la imagen de la entidad y ningún funcionario está autorizado para alterar la forma o la información contenida, teniendo en cuenta que la firma tendrá la siguiente información:
    - Nombre, cargo, empresa, número de contacto corporativo, direcciones físicas, página web, correo electrónico de contacto, logo del canal y política de confidencialidad de información.
- Garantizar que se mantengan los correos electrónicos procesados por todos los sistemas e infraestructuras tecnológicas que maneje Televisión Regional del Oriente.

RESPONSABILIDADES: funcionarios, contratistas y terceros vinculados a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADOS CLAVES: Dar cumplimiento a los lineamientos expuestos en la política de uso de correo electrónico.

5.2 POLITICA DE ESCRITORIO Y PANTALLA LIMPIA

RESUMEN: Esta política establece las normas a tener en cuenta por parte de empleados y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, para el correcto manejo de documentos e información que se encuentren en los puestos de trabajo y equipos de cómputo durante y fuera del horario laboral evitando acceso no autorizado, perdida, daño y robo de información.

INTRODUCCIÓN: Para tener un adecuado aseguramiento de la información que está bajo la responsabilidad de los empleados y contratistas de TELEVISIÓN

REGIONAL DEL ORIENTE LTDA. CANAL TRO se debe contar con una política de escritorio limpio y pantalla limpia, adoptando buenas prácticas que permitan el correcto manejo de la información física y digital propia de la identidad que pueda ser alcanzada, copiada, no respalda o utilizada por terceros o por personal que no tenga autorización para uso o conocimiento.

ALCANCE: Esta política se aplica a todos los usuarios o trabajadores de la organización, dicha política sustenta la organización de la información, además, se aplica a todos los puestos de trabajo, instalaciones y equipos de cómputo y periféricos ubicados dentro de la entidad. Los usuarios de este documento son todos los empleados, contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer lineamientos que permitan prevenir la pérdida, daño, robo o compromiso de la información durante y fuera de las horas laborales en los puestos de trabajo y equipos de cómputo de los funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIOS: TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO sensibiliza a todos los funcionarios y contratistas para que adopten la política de escritorio y pantalla limpia realizando seguimiento de las directrices estipuladas para que se aborden siempre que sea necesario.

- Los sitios de trabajo de los empleados y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, deben localizarse en ubicaciones donde no queden expuestos al acceso de personas externas.
- Al ausentarse el empleado o contratista de su puesto de trabajo debe guardar en un lugar seguro y bajo llave cualquier documento físico, medio magnético u óptico que contenga información pública de uso interno, clasificada o reservada al igual bloquear la sesión en su equipo de cómputo.
- Al finalizar la jornada laboral los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan cualquier tipo de información, estas deben guardarse en un lugar seguro y bajo llave.
- Los puestos de trabajo deben permanecer limpios y ordenados.
- Cuando se imprima o digitalice documentos estos deben retirarse de los equipos periféricos.
- Los gabinetes, cajones y archivadores que contengan documentos y/o medios extraíbles deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral.
- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que empleados y contratistas cumplan con sus actividades diarias.

- Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.
- Si se utiliza un equipo portátil, debe mantenerse en un lugar seguro para evitar hurto del equipo.
- No dejar dispositivos extraíbles (USB, CD, DVD, Disco Duro Externo, etc) con información en lugares visibles o accesibles.
- Cualquier equipo portátil debe ser debidamente asegurado si se va a dejar desatendido. Es necesario guardarlo bajo llave
- Todo el personal debe conocer y rendir cuentas por la seguridad de la información en cuanto sea pertinente para su rol de trabajo.
- Se debe implementar un modelo estándar de protector y fondo escritorio institucional en las pantallas de los equipos de cómputo de forma que se active tras un periodo de inactividad.

RESPONSABILIDADES: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADOS CLAVES: Dar cumplimiento a la política de escritorio y pantalla limpia.

5.3 POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

RESUMEN: Este documento define las políticas que se deben aplicar para la protección de los activos de información de la TELEVISIÓN REGIONAL DEL ORIENTE a través de un proceso de clasificación de acuerdo a su nivel de importancia y sensibilidad.

INTRODUCCIÓN: Se considera información todo tipo de datos generados de manera digital, escrito en papel, formularios, o transmitido mediante una red de datos o dispositivos móviles de almacenamiento, lo cual constituye un estado de conocimiento.

Un activo de información es un elemento definido e identificado que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como valiosa para TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO; independiente del tipo de activo, es necesario considerar las siguientes características:

- Los activos no son fácilmente reemplazables y su alteración o daño representa costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.

- Los activos forman parte de la identidad y su vulnerabilidad puede poner en riesgo las operaciones misionales y/o estratégicas de TELEVISIÓN REGIONAL DEL ORIENTE CANAL TRO.

ALCANCE: Los Lineamientos de esta política deben ser aplicados a todos los funcionarios y contratistas que tengan uso directo de los activos de información de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer, clasificar y valorar los activos de información para que a través de unos lineamientos que me permitan mantener actualizada la adecuada identificación y clasificación de los activos de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIOS

- Se identifican los activos de información de mayor importancia asociados a cada Sistema de Procesamiento de la Información en su respectivo proceso, con sus responsables y su Ubicación, para luego elaborar un inventario con dicha información.
- El Inventario se deberá identificar, documentar y actualizar ante cualquier modificación de la información y los Activos asociados con los Medios de Procesamiento. Este debe ser revisado con una periodicidad no mayor a un (1) año.
- La responsabilidad de realizar y mantener actualizado el inventario de activos de información es de cada responsable de proceso de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- El uso de los activos de información pertenecientes a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO es responsabilidad del propietario asignado; es su deber proteger y mantener la confidencialidad, integridad y disponibilidad de los activos de información teniendo en cuenta el nivel de riesgo que ese activo tiene de acuerdo a su clasificación, y abstenerse de almacenar en ellos información no organizacional.
- Una vez se dé por terminada la relación con un empleado, cliente, contratista o tercero, se le deben retirar todos los privilegios de acceso a los recursos institucionales del canal y la persona deberá realizar la devolución de los activos que le hayan sido asignados o se encontrasen bajo su custodia durante su vinculación al canal.
- El responsable de cada proceso es el encargado de realizar la gestión para el retiro de acceso a los recursos institucionales que acarree la desvinculación de un cliente, empleado, contratista o tercero.
- Los colaboradores, contratistas, y en general los usuarios de la red, responsables de la información de TELEVISIÓN REGIONAL DEL ORIENTE

LTDA. CANAL TRO, deben identificar los riesgos a los que está expuesta la información, teniendo en cuenta que esta pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo. Por lo tanto, se debe custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar su sustracción, destrucción, o uso indebido.

- Los procedimientos de seguridad de la información están bajo la responsabilidad de los líderes de área y estos deben asegurarse de que todos los miembros del grupo cumplan con las políticas y estándares de seguridad de la información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

- Los líderes de las diferentes áreas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO son los responsables de mantener actualizado el inventario de los activos de información.

- Los empleados, contratistas y terceros no podrán revelar a personas ajenas a la organización la información a la que tengan acceso en el ejercicio de sus funciones, de acuerdo con la guía de clasificación de la información y según sus niveles de seguridad.
- Las conexiones directas con los sistemas de cómputo y comunicaciones de otras entidades, a través de Internet o cualquier otro tipo de red, deben contar con una autorización previa, basada en un análisis de riesgos de seguridad de la información.

RESPONSABILIDAD: funcionarios, contratistas y terceros vinculados con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO

RESULTADOS CLAVES: Establecer, clasificar y valorar todos los activos de la información de TELEVISIÓN REGIONAL DEL ORIENTE CANAL TRO.

5.4 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE LA INFORMACIÓN

RESUMEN: El presente documento establece los lineamientos aplicables a los sistemas de información y a la infraestructura de servidores de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO en lo referente al respaldo y restauración de información.

INTRODUCCIÓN: Cualquier dispositivo de almacenamiento masivo tiene la posibilidad de fallar por esto, TELEVISIÓN REGIONAL DEL ORIENTE LTDA.

CANAL TRO ha determinado la necesidad de contar con una política de respaldo y restauración de información garantizando la disponibilidad e integridad de la información al administrador y líder de servicio de tecnología para reducir el impacto de los riesgos generados en fallas de prestación de servicio que involucren la pérdida total o parcial de la información.

ALCANCE: Esta política aplica a todos los funcionarios y contratistas que sean responsables de administrar la infraestructura tecnológica, sistemas de información y dispositivos de almacenamiento masivo que contengan información de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO para la prestación del servicio.

OBJETIVO: Definir lineamientos que permitan tener un correcto respaldo y restauración de información con el fin de preservar la integridad, confidencialidad y disponibilidad de la información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIOS

- TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO adoptará planes de recuperación de emergencia para todas las aplicaciones que manejen información crítica, y sean responsabilidad de la entidad. Dichas copias se actualizarán periódicamente, y se verificará el respaldo correcto.
- TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO mantendrá al menos una copia de la información en un servidor de archivos ubicado en el (Data center) de la entidad, esto para las aplicaciones de tipo local, para aquellas que están en la nube, se realizará un proceso de copia de respaldo si aplica.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información. A su vez, se realizarán periódicamente pruebas de funcionamiento y ejecución de los procesos de *backup*.
- Las copias de las bases de datos de los servidores de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO se harán de forma automática o manual, según el sistema de información; las bases de datos se deben sacar con discos duros extraíbles que siempre permanecerán en el sitio y se eliminará la información cada cuatro meses con el fin de generar espacio de almacenamiento efectuando un proceso de borrado seguro y posteriormente la eliminación o destrucción en forma adecuada.
- Los storage de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO deben de garantizar una configuración tipo RAID a nivel de infraestructura que permita un respaldo automático de información en dado caso que se presente una falla en disco duro del arreglo.
- Los respaldos de información sensible, crítica y valiosa deben almacenarse en un sitio protegido contra inclemencias del medio ambiente y con controles

estrictos de acceso que se encuentre a una distancia razonablemente fuera del alcance de un evento en la zona original.

- Todos los colaboradores de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO conocerán la información que deben respaldar según su rol de trabajo.
- Se harán reportes de la información a la que se les realizó backups.
- No serán tolerables pérdidas de información por la inexistencia del backup de la misma.
- Todas las copias de información crítica de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO deben almacenarse en un área adecuada y con un control de acceso. Estas copias se mantendrán con el propósito de tener un respaldo y restauración de los sistemas en caso de la materialización de una amenaza, como pueden ser: defecto en los discos de almacenamiento, problemas en los servidores y computadores, virus o ataques informáticos, catástrofes naturales o provocadas por el hombre.
- Los administradores de los servidores de backups (tercerizado) realizarán periódicamente pruebas de restauración de la información mediante la rotación de los medios y en un ambiente de pruebas controlado, si aplica.
- Los usuarios deberán estar conscientes de que la información confidencial o sensible almacenada en sus computadoras puede ser recuperada con métodos avanzados aun cuando haya sido “normalmente” borrada. Por esta razón se deberán tener las precauciones para el manejo de información Confidencial en las computadoras y memorias USB, que hayan tenido esta información y que se pretendan prestar o compartir.

RESPONSABILIDAD: funcionarios y contratistas de la TELEVISION REGIONAL DEL ORIENTE

RESULTADOS CLAVES: Dar cumplimiento a la política de respaldo y restauración de información.

5.5 POLÍTICA DE USO DE INTERNET

RESUMEN: La política de uso de internet, proporciona a los empleados el lineamiento acerca del uso apropiado de los equipos, la red y el acceso a internet de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, con el fin de proteger tanto a la entidad como al empleado y/o contratista.

INTRODUCCIÓN: Internet es un recurso limitado y, por lo tanto, el uso debe ser para el interés de las actividades de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, toda información transmitida por este medio será tratada como información relacionada con la entidad.

ALCANCE: La presente política es aplicable a funcionarios, contratistas y terceros vinculados con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer lineamientos que permitan tener un buen uso de internet para optimizar y facilitar funciones propias de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIO

- Establecer normas que aseguren el buen funcionamiento de Internet, para optimizar y facilitar sus labores de trabajo en TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Establecer las normas que regulen el uso aceptable del servicio institucional de Internet por parte de los funcionarios y contratistas de la entidad, personal externo, terceros y/o pasantes autorizados, considerando al servicio de Internet como una herramienta de apoyo en la gestión y desempeño de sus funciones y actividades laborales.
- Proteger la Información almacenada en los computadores dentro de la infraestructura de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, evitando así las amenazas latentes por el uso indebido del servicio de Internet.
- La divulgación de información confidencial de la entidad en grupos de discusión, listas o chats está prohibida, independientemente si esta fue deliberada o involuntaria. Serán aplicadas las sanciones previstas en las políticas y procedimientos internos según lo dispuesto por la ley.
- Los colaboradores con acceso a Internet solo pueden descargar programas directamente vinculados a las actividades de la entidad y deben proporcionar lo que sea necesario para regular la licencia y el registro de dichos programas.
- Los colaboradores con acceso a Internet no podrán cargar ningún software con licencia o los datos que sean propiedad de la entidad sin el permiso expreso del gerente o responsable de TI.
- En esta organización no se permitirá el software de comunicación instantánea como Skype, WhatsApp y similares sin la debida autorización por parte del responsable de TI.
- Todo el personal debe conocer que no se permitirá el uso de software para descargar música, videos y otro contenido en formato Torrent.
- No se permitirá el uso de servicios de transmisión como Radios en línea o similares.
- El uso de las redes sociales se permitirá solo a los usuarios cuya actividad final, dependa de este tipo de acceso.
- Los usuarios de los servicios de internet de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO deben hacer uso razonable de estos recursos y solo con propósitos laborales.

- No se permite la navegación a sitios con contenidos que representen peligro para la entidad como pornografía, terrorismo, *hacktivismo*, Deep web, segregación racial u otras fuentes asociadas a estos riesgos.
- Los usuarios de la red deben ser conscientes del uso adecuado de internet, y deben evitar el acceso a sitios potencialmente peligrosos o que puedan afectar el buen desempeño de la red.
- El responsable de TI inhabilitará el acceso a sitios web identificados como peligrosos, de alto consumo de recursos de red, o que afecten el desempeño del personal, a fin de proteger y no comprometer la seguridad y el desempeño de la red y los recursos informáticos de la entidad.
- La descarga de archivos de internet debe hacerse con propósitos laborales y de forma razonable para no afectar el servicio de Internet y la red de datos en general.
- No se permite la descarga por Internet de archivos que puedan afectar el rendimiento de la red y uso del enlace de Internet. (.exe, p2p, peliculas, video juegos, etc.)
- Cumplir las normas de uso aceptable del servicio institucional de Internet definidas en la presente Política.
- Cumplir con los procedimientos de autorización de servicios y recursos tecnológicos establecidos para tal efecto.
- Utilizar el servicio institucional de Internet, para asuntos relacionados con el desempeño de las funciones laborales o contractuales asociadas a la entidad TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Los usuarios de servicios de internet de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO deben hacer uso razonable de los elementos y servicios suministrados por la entidad, además de utilizarlos sólo para propósitos laborales.
- No se podrá utilizar los recursos de la entidad para descargar o distribuir software o datos no legalizados.
- Habrá bloqueo de acceso para archivos o dominios que comprometan el uso del ancho de banda o que interrumpan el buen funcionamiento de las labores del canal.

RESPONSABILIDAD: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADO CLAVE: Dar cumplimiento a la política de uso de internet.

5.6 POLÍTICA DE REPORTE DE INCIDENTES DE SISTEMAS DE INFORMACIÓN

RESUMEN: Esta política establece a través de un modelo propuesto el reporte de incidentes de seguridad de la información y el manejo adecuado que se le deba dar al interior de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO

INTRODUCCIÓN: Se entiende como incidente de seguridad, cualquier evento que ponga en riesgo la integridad, disponibilidad y confidencialidad de la información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO; Esta política contiene los componentes generales de la gestión de incidentes de seguridad y sus principales acciones, las cuales son aplicables en toda la organización y en toda información o activo de información sobre el cual se presente o exista un indicio de incidente de seguridad, generando confianza y responsabilidad en reportes de incidentes de seguridad de la información que se presenten en la entidad.

ALCANCE: Esta política es aplicable a todos los funcionarios, contratistas y terceros que detecten un evento o incidente de seguridad de la información, el cual deben reportar adecuadamente según los lineamientos establecidos por la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer normas que permitan dar gestión a los incidentes de riesgo de seguridad de la información advirtiendo y mitigando el impacto de los mismos.

PRINCIPIOS

- Dar a conocer los lineamientos generales definidos por Seguridad de la Información, para el manejo de los posibles incidentes de seguridad de la información que puedan presentarse al interior de la entidad.
- Generar un compromiso con los empleados de realizar el reporte al momento de ocurrir cualquier incidente de seguridad de la información al interior o con las aplicaciones propias de la entidad
- Establecer la afectación del activo de información, incluyendo el valor económico y la cantidad de información relevante para la entidad contenida en el mismo.
- Todo el personal de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO debe estar vigilante respecto a los incidentes (incluyendo fallas en el sistema, pérdida del servicio, errores resultados de datos incompletos o inadecuados, rompimiento de la confidencialidad). Si se detectan estos incidentes o debilidades de seguridad, deben ser reportados en forma inmediata al encargado de seguridad al email: direccion. tecnica@canaltro.com
- Los usuarios son la primera línea con la que se pueden identificar eventos adversos sobre la información o algún activo de información, y es de su responsabilidad y deber reportar cualquier situación anormal que pueda llegar a convertirse en un incidente de seguridad de la información.

- Un colaborador, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad, debe notificarlo a la mesa de ayuda quién será el primer punto de contacto.
- El encargado de la seguridad de la información es el responsable de coordinar los esfuerzos necesarios para dar atención a un incidente dentro de la entidad, de igual manera, tiene la responsabilidad de informar a los respectivos niveles administrativos de los incidentes y su grado de severidad dentro de la entidad, así como coordinar los esfuerzos con empresas externas en caso de ser necesario.

RESPONSABILIDAD: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADO CLAVE: Dar cumplimiento a la política de reporte de incidentes de los sistemas de información.

5.7 POLÍTICA DE ADMINISTRACIÓN DE CONTRASEÑAS

RESUMEN: Esta política establece las pautas necesarias para la creación correcta y segura de una contraseña, la protección y el cambio cada cierto tiempo de la misma, mejorando la seguridad en los sistemas de información buscando una mejor protección de los datos en TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

INTRODUCCIÓN: Las contraseñas son un aspecto muy importante de la Seguridad de la Información. Una contraseña débil puede dar lugar a accesos no autorizados y/o explotación de recursos de la entidad. Todos los usuarios, incluyendo contratistas y proveedores con acceso a sistemas de la entidad, son responsables de tomar las medidas adecuadas para seleccionar y proteger sus contraseñas.

ALCANCE: Esta política se aplica a todo el personal que tenga asignada una contraseña para el inicio de sesión de cualquier herramienta de software que maneje la organización TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer un estándar de uso de contraseñas seguras, la protección de las mismas y su frecuencia de cambios.

PRINCIPIO

- TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO verificará el cumplimiento de esta política a través de diversos métodos, incluyendo, pero no limitado a, revisiones periódicas, video vigilancia, informes de la herramienta de negocio, auditorías internas y externas, así como la retroalimentación al dueño de la política.

- Todo empleado que sea hallado como transgresor de esta política puede estar sujeto a medidas disciplinarias, que pueden incluir hasta terminación del contrato, dependiendo de la gravedad de la falta.
- No se debe permitir que individuos que no sean miembros de la entidad tengan acceso a los servicios de cómputo y comunicaciones de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO. Todos los funcionarios, contratistas y terceros deben velar porque este tipo de situaciones no se presenten al interior de la entidad.
- Cada contraseña es de uso personal e intransferible. Los colaboradores no deben revelar la contraseña de su cuenta a otros y/o terceros. Se debe notificar inmediatamente al responsable de TI si sospechan que alguien ha obtenido acceso sin autorización a su cuenta y debe modificarla en forma inmediata. Cualquier excepción a la norma debe ser aprobada por el personal encargado de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO con antelación.
- Está prohibido enviar la contraseña por el correo electrónico, (teniendo en cuenta que este no es un medio seguro) o mencionarla en una conversación
- Para el buen uso de las contraseñas se debe tener en cuenta los siguientes aspectos:

  - Las contraseñas deben ser construidas con mínimo ocho (8) caracteres
  - Deben Incluir mayúsculas, minúsculas, números y caracteres especiales.
  - No utilizar contraseñas que sean únicamente palabras o nombres (aunque sean extranjeras).
  - No utilizar contraseñas completamente numéricas con algún significado (teléfono, fechas, direcciones, nombres, lugares).
  - Cambiar la contraseña 4 veces al año; cada 3 meses.

RESPONSABILIDADES: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
RESULTADO CLAVE: Dar cumplimiento a la política de administración de contraseñas.

5.8 POLÍTICA DE PROTECCIÓN CONTRA CODIGO MALICIOSO

RESUMEN: El presente documento establece los lineamientos necesarios para la protección adecuada contra código malicioso; detectando, previendo y recuperando información contra un código no autorizado.

INTRODUCCIÓN: El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos. La Gestión Técnica de Canal

TRO deberían, cuando sea apropiado, introducir controles para evitar, detectar y retirar los códigos maliciosos.

ALCANCE: El alcance de los lineamientos que se definen en esta política da cubrimiento a los accesos que involucren:

- Hardware (servidores, equipos de cómputo portátiles y de escritorio, medios de almacenamiento externo, como memorias externas USB, CD (Discos Compactos) y DVD.
- Software no autorizado por el área de TI.
- Acceso a internet.
- Red interna (Intranet)

OBJETIVO: Establecer lineamientos que permiten un control adecuado contra código malicioso.

PRINCIPIO

Definir las medidas de prevención, detección y corrección frente a amenazas causadas por códigos maliciosos en TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

- Está prohibida la descarga y/o instalación de software no autorizado. Si se necesita instalar programas que no se encuentren en la lista autorizada se deberá contar con autorización del administrador de TI. La lista de software autorizado se encuentra dentro de cada documento de los diferentes cargos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.
- La red de servidores y computadores de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO deberá tener instalada una plataforma de hardware y software de ANTIVIRUS para evitar la propagación de software malicioso.
- La plataforma de ANTIVIRUS debe cumplir los siguientes requerimientos:
    - Consola centralizada de administración.
    - Actualización de la base de datos de virus o amenazas para los antivirus de forma permanente, automática y centralizada.
    - Distribución de actualizaciones automática de las estaciones de trabajo.
    - Monitoreo centralizado.
    - Debe verificar la presencia de código malicioso en todos los archivos en ordenadores, dispositivos magnéticos y servidores.
    - Debe verificar la presencia de código malicioso en los adjuntos y las descargas del correo electrónico antes del uso, esta verificación se

debe efectuar en los servidores de correo electrónico, los ordenadores y cuando ingresan a la red de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
  - Debe verificar las páginas web para comprobar la presencia de código malicioso.
  - Bajo impacto en los tiempos de respuesta de las estaciones.
  - Proteger la totalidad de los computadores, servidores y equipos de la red para TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO
  - Capacidad del Antivirus para ejecutarse en los diferentes sistemas operativos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Todos los colaboradores y terceros que hacen usos de los servicios prestados por TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO son responsables de manejo de antivirus para analizar, verificar y (si es posible) eliminarlos de la red, computadores, dispositivos de almacenamiento fijos, removibles, archivos, correos electrónicos que estén utilizando para el desempeño de sus funciones laborales.
- La instalación y manipulación del antivirus sólo puede realizarse por el responsable de TI
- Todos los equipos conectados a la red TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO pueden ser monitoreados y supervisados por la oficina de TI.
- Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.
- Se deben llevar a cabo revisiones (mensuales, semestrales) del software y del contenido de datos de los sistemas. Se debe investigar la presencia de archivos no aprobados o modificaciones no autorizadas.
- El responsable de TI deberá recolectar y estar actualizado con información de diferentes tipos de malware y de cómo minimizar la probabilidad de infección.
- Se deben hacer campañas de sensibilización a todos los trabajadores, colaboradores, terceros y clientes de ser el caso que no cuenten con políticas propias de control de código malicioso, con el fin de generar una cultura de seguridad de la información y minimizar los riesgos. Estas campañas están compuestas por:
  - Capacitaciones de concientización al ingreso de nuevo personal, y de manera anual al personal vigente.
  - Sensibilización de los diferentes tipos de malware y cómo prevenir una infección.
- Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, cuyo origen sea

desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta establecida para ello.

- Los sistemas de cómputo que se sospechen han sido comprometidos por virus o software malicioso deben ser apagados y desconectados de la red en forma inmediata. El usuario debe solicitar apoyo técnico e informar al líder de área.

- Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

- Antes de restaurar archivos desde copias de respaldo, dichas copias deben ser evaluadas con el software antivirus de la entidad.

- Concienciación y formación del personal.
- Instalar y actualizar un sistema de antivirus e instaurar una política para utilizarlo con los ficheros adjuntos en un correo electrónico o con los que descargamos.
- Crear procedimientos para usar el antivirus, dar formación para su uso y para afrontar ataques.

RESPONSABILIDAD: funcionarios y contratistas vinculados a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADO CLAVE: Dar cumplimiento a la política de protección contra código malicioso.

5.9 POLÍTICA DE ACCESO FÍSICO AL DATA CENTER

RESUMEN: La presente política establece las reglas para acceso físico al centro de datos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, teniendo en cuenta su acceso por funcionarios y/o contratistas autorizados, con videovigilancia, sistema de alarma y detección de incendios.

INTRODUCCIÓN: La seguridad física de la data center de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO implica proteger la infraestructura critica de amenazas externas o intrusiones que atente contra las actividades de la entidad.
La seguridad física de los data centers implica proteger la infraestructura crítica de amenazas externas o intrusiones que atenten contra las actividades de una

empresa. Elementos de alto valor y sumamente importantes, tales como servidores, switches y unidades de almacenamiento.
Este tipo de seguridad incluye videovigilancia a través de cámaras, sistemas de control de acceso y seguridad perimetral.

ALCANCE: Esta política va dirigida a funcionarios y contratistas que tengan acceso a la infraestructura de la data center de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Definir lineamientos que permitan un acceso seguro y adecuado a la infraestructura de la data center de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIO

- Para un acceso seguro se debe tener un usuario y contraseña registrados en forma previa, es responsabilidad del usuario velar por la confidencialidad de la credencial de acceso.
- Hay sistemas de video vigilancia, la actividad dentro de los centros de datos y perimetral en la entidad en controlada y grabada en servidores seguros (DVR).
- Con el fin de controlar y supervisar el acceso a los centros de datos, cada miembro del personal tiene una placa RFID (Tarjeta de identificación mediante radio frecuencia) nominal para restringir su acceso.
- Los derechos de acceso de los colaboradores son supervisados regularmente.
- El fuego es otro riesgo controlado. Cada sala del centro de datos está equipada con detectores de fuego y sistemas de extinción, así como puertas cortafuego. Los data centers cumplen con la norma APSAD R4 para la instalación de extinguidores, además cuenta con la certificación N4 de conformidad.

RESPONSABILIDAD: funcionarios y contratistas vinculados con la televisión regional del oriente

RESULTADO CLAVE: Dar cumplimiento a la política de acceso físico a la data center de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

5.10 POLÍTICA DE MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

RESUMEN: Esta política establece normas para un adecuado análisis de requerimientos y controles para el desarrollo y mantenimiento de sistemas de información que brindan soporte a los procesos de la organización.

INTRODUCCIÓN: El desarrollo y mantenimiento de sistemas de información conlleva una serie de etapas que definen el flujo de actividades que se ejecuten con buenas prácticas para beneficio de la información propia de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

ALCANCE: Esta política va dirigida a funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO que tengan la responsabilidad del desarrollo y mantenimiento de los sistemas de información de la entidad.

OBJETIVO: Establecer lineamientos que permitan el fortalecimiento y correcto y mantenimiento de los sistemas de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO y cualquier software que contenga información.

PRINCIPIO

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos de la organización.
- El responsable de la seguridad de la información debe identificar y sugerir los controles a ser implementados en los sistemas desarrollados internamente o por terceros
- Verificar el cumplimiento de los controles establecidos para el desarrollo y Mantenimiento de sistemas.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas.
- El líder del área TI es el responsable de la administración de las técnicas criptográficas y claves; licenciamientos, calidad del software y la seguridad de la información en los contratos con terceros para desarrollo de software.

RESPONSABILIDAD: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO

RESULTADO CLAVE: Dar cumplimiento a la política de desarrollo y mantenimiento de sistemas de información

5.11 POLÍTICA DE CONFIDENCIALIDAD DE LA INFORMACIÓN

RESUMEN: Esta política establece los requisitos bajo los cuales cada uno de los miembros de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO deben tratar la información (Pública, interna y reservada) originada en el ámbito de la misma protegiéndola de su divulgación NO autorizada a terceros.

Se considera información confidencial:

- Información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO declarada como confidencial e información entregada por terceros bajo un acuerdo de confidencialidad.
- Datos de funcionarios, contratistas o terceros relacionados con la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO que no hayan sido difundidos públicamente.
- Documentación relacionada con las actividades de las distintas áreas de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO que no haya sido difundida públicamente por la misma.

INTRODUCCIÓN: La confidencialidad es la seguridad de que la información será protegida y no divulgada sin la aprobación del propietario de dicha información. La información que TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO declare como confidencial se regirá por un conjunto de reglas que limiten el acceso a la información.

ALCANCE: Esta política es aplicable a funcionarios y contratistas de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO y se refiere a las acciones individuales o conjuntas realizadas por o en nombre de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer reglas que permitan la protección de los datos que tiene, maneja y dispone los funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIOS

- TELEVISIÓN REGIONAL DEL ORIENTE CANAL TRO ha adoptado un sistema de clasificación de la información que categoriza la información en tres grupos de acuerdo a su grado de confidencialidad. Toda la información bajo control de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, sea ésta generada interna o externamente, se encuentra en una de estas categorías: Público, Interno y Reservado.

- Todos los funcionarios y contratistas deben familiarizarse con las definiciones para estas categorías y cumplir con las medidas de protección establecidas para ellas.
- Si la información no está clasificada como pública, ésta no podrá ser proporcionada a ninguna entidad externa sin un acuerdo de confidencialidad.

- Los funcionarios, contratistas y terceros que trabajan para TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, en ausencia de instrucciones claras o precisas, considerarán la información como de uso interno exclusivamente. Esta política aplica especialmente cuando, por algún motivo, no se ha realizado una clasificación de la información.

- Toda la información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO (Pública, Interna y Reservada) debe estar protegida para evitar que personas no autorizadas la consulten, divulguen o modifiquen sin consentimiento.

- Si se confirma o se sospecha que la información o datos confidenciales o privados, son extraviados o revelados a empresas no autorizadas, el Propietario de la información o quien evidenció el hecho deberá notificar inmediatamente al encargado de la seguridad informática de la entidad con el objeto de realizar un control efectivo de posibles daños y tomar las acciones necesarias.

- No se revelarán los controles de seguridad de los sistemas de información y la forma en que están implementados. Esto incluye: Información que se proporciona en presentaciones, discusiones, o es tratada en diferentes foros que incluya aspectos técnicos de infraestructura.

- Toda información clasificada debe ser etiquetada (marcada) con base en estándares definidos. Se buscará que estas etiquetas sean mantenidas en buen estado y visibles de tal forma que se puede identificar la clasificación de la información de la entidad en cualquier momento.

- Toda la documentación impresa, escrita a mano o documento legible que contenga información clasificada como confidencial o de uso interno, debe tener una etiqueta que indique el nivel apropiado de sensibilidad con base en la clasificación.

RESPONSABILIDADES: funcionarios, contratistas y terceros que tengan vínculo con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADOS CLAVES: Dar cumplimiento al tratamiento de la información de acuerdo a su tipo de clasificación (publica, interna y reservada).

5.12 POLÍTICA DE GESTIÓN DE CLAVES DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

RESUMEN: Esta política hace referencia a los parámetros que garantizan el adecuado control en la protección de los sistemas de información mediante la vigilancia de acceso a la información almacenada en cualquier medio (físico/digital) propio de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

INTRODUCCIÓN: TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO identifica la información como un componente indispensable para la organización, por esta razón establece el control de acceso lógico como la primera línea de defensa de ingreso de personas no autorizadas a información propia de la entidad. Para controlar el acceso se emplean 2 procesos: identificación y autenticación.
La identificación se entiende como el momento en que el usuario se da a conocer en el sistema; y autenticación a la verificación que realiza el sistema sobre esa identificación por medio de contraseñas con un nivel alto de seguridad que solo manejen usuarios con sus respectivos roles. Para la elaboración del mismo se toman en cuenta las regulaciones aplicables según el sistema de seguridad de la entidad y la política de administración de contraseñas.

Para TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO es prioritario definir el personal que tenga acceso a información sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la información puede ser sensible o tener un carácter confidencial. Así mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de la misma.
La plataforma tecnológica es responsabilidad del área técnica, así como los sistemas de información de la Entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso pertinentes a dichos recursos.

Área técnica es responsable de garantizar entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en oficinas, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

ALCANCE: Esta política aplica para todos los funcionarios, contratistas y terceros que tengan acceso a toda la información contenida en cualquier medio (digital o

físico), áreas de procesamiento de información, redes de datos, recursos de la plataforma tecnológica y sistemas de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer lineamientos que permitan la adecuada gestión de control de acceso lógico a las áreas de procesamiento de información, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO manteniendo la confidencialidad, integridad y disponibilidad de la información.

PRINCIPIOS

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

- Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud al área respectiva.

- Se deberán realizar revisiones periódicas en los diferentes sistemas de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo una vez al mes.

- Cada miembro del personal de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.
- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

    - El jefe de área o líder de proceso deberá ser el único autorizado para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario, a través de las diferentes categorías de la mesa de ayuda.

- Sensibilizar a los usuarios en cuanto a la responsabilidad en el uso de las buenas prácticas de seguridad en la selección, uso y protección de las credenciales de acceso a los sistemas de información con el fin de preservar la integridad de la información.
- Garantizar el uso de herramientas seguras cuando se trabaje de forma remota.

- Todos los colaboradores deben tomar medidas de seguridad, terminando las sesiones activas cuando finalice su actividad o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
- Las contraseñas no deben ser reveladas a ninguna persona, y no deben ser registradas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y que el método de almacenamiento esté aprobado por el comité respectivo.
- Las cuentas de usuario y contraseña de administradores son de uso personal e intransferible, con su respectivo respaldo bajo herramientas seguras en el director de área y gerencia.
- Los sistemas de información deben tener un protocolo para recuperar las contraseñas en dado caso que se presente algún siniestro.
- Se tomarán acciones cuando se afecte la información debido a la omisión de alguna de las políticas anteriores; de igual manera cuando por una mala gestión de contraseñas los resultados no sean los deseados.
- Los usuarios de la red de datos son los directamente responsables del uso de las claves o contraseñas de acceso que se le asignen, o ellos mismos establezcan para la utilización de los equipos y/o servicios informáticos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar el procedimiento de resguardo y custodia de las claves o contraseñas en un sitio seguro, utilizando herramientas que permitan la protección de dichas claves. A esta herramienta solo debe tener acceso el responsable de asignación de contraseñas y la gerencia del canal.
- Funcionarios, contratistas y terceros deben emplear obligatoriamente contraseñas con un alto nivel de complejidad de acuerdo con el rol asignado y la importancia de la información que maneje.
- En toda la política se tendrá en cuenta las posibilidades de fraude asociado al abuso de los sistemas de información.

- Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.
- Se deberá deshabilitar o borrar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

- La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación (sistema) y de las áreas responsables de dicho activo.

- El jefe de área o Líder de proceso deberá establecer los permisos que corresponde a cada perfil que puede acceder a los recursos de la plataforma tecnológica, servicios de red y los sistemas de información.

- Los administradores de cada aplicación (sistema) deberán crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por el jefe de área o líder de proceso.

- Se deberá establecer un procedimiento de entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, a los recursos de la plataforma tecnológica o a los sistemas de información.

- Se deberán inhabilitar o eliminar los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica.

- Se deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

- Se deberá establecer controles de acceso a los ambientes de producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados para garantizar el acceso a la información.

- Se deberán establecer mecanismos de auditoria al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.
- Se deberá identificar al personal que requiere acceso a las instalaciones de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, autorizar su ingreso y conceder los privilegios necesarios para el acceso físico.

- Se deberá contar con mecanismos de control de acceso para las áreas seguras (el centro de cómputo, la unidad de diagramación administración de infraestructura y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO considere pertinentes.

- Las puertas de acceso al centro de cómputo, unidad de diagramación, administración de infraestructura, y centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.

- Se deberá aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura, unidad de diagramación o a los centros de cableado, además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.

- Se deberá registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado en una bitácora ubicada en la entrada de estos lugares de forma visible.

- Se deberá monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

- Se deberá bloquear de manera inmediata los privilegios de acceso físico a las instalaciones de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO tan pronto el personal termine su vinculación.

- Se deberá realizar la devolución del carné institucional tan pronto el personal termine su vinculación con TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

- Se deberá implementar controles de acceso físico al centro de cómputo para evitar la manipulación no autorizada del cableado.

RESPONSABILIDADES: funcionarios, contratista y terceros vinculados con la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADOS CLAVES: Dar cumplimiento a los lineamientos de la política de claves de acceso a los sistemas de información.

5.13 POLÍTICA DE USO DE LOS ACTIVOS DE INFORMACIÓN

RESUMEN: La presente política de uso de los activos de la información busca crear lineamientos que permitan la adecuada protección de los datos e información relevante para TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, implementando controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información por ello se debe concientizar a todos los funcionarios, contratistas y demás colaboradores sobre un manejo seguro y adecuado de los activos de información.

INTRODUCCIÓN: La información es uno de los activos más valiosos de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO debido a esto los empleados y contratistas que hacen uso de los activos que llevan esta información deben tener un alto nivel de compromiso siempre orientados al cumplimiento de la misión de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO es el propietario principal de los activos de información. Así mismo, los administradores de estos activos son los funcionarios y contratistas de la entidad y son ellos las personas autorizadas y responsables de la información generada en los procesos a su cargo, así como de los sistemas de información o aplicaciones informáticas, hardware o infraestructura tecnológica que tengan a su cargo.

ALCANCE: Esta política es aplicable a funcionarios, contratistas y terceros que hagan uso de los activos de información pertenecientes a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer normas que permitan mantener la confidencialidad, integridad y disponibilidad de los activos de información buscando como prioridad la protección y el correcto uso de los activos de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIO

- No se pueden almacenar, instalar o utilizar software no autorizado en los equipos de cómputo de escritorio, y dispositivos móviles de la entidad; de igual manera, no se podrán realizar cambios, ajustes o mejoras en la infraestructura física o lógica de aplicaciones instaladas en dichos equipos.
- Todo el personal debe conocer y rendir cuenta por aplicar un mal uso de los activos de información. Estos actos incluyen él envió de correo electrónico masivo con fines no organizacionales, prácticas de juegos en línea, consultas a sitios web no permitidos, entre otros.
- Se hará seguimiento al correcto uso de los activos de la información.
- Se tomarán acciones cuando los activos de la información no estén dando resultados aceptables.
- No se tolerarán situaciones que puedan poner en riesgo la organización y que no vayan de acuerdo a lo dicho en esta política.
- El responsable de TI a través del proveedor de servicio de internet realizará el aseguramiento de los accesos a internet, a redes de terceros y de la entidad; este compromiso incluye —pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos prevenir la introducción y propagación de virus, dada la constante evolución de nuevos ataques cibernéticos a los que están expuestos los sistemas de información.
- El líder de cada proceso gestionará ante el responsable de TI los cambios o modificaciones que se deban hacer sobre la infraestructura tecnológica.
- Los usuarios de los activos de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO son los responsables de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Los usuarios de la red de datos deberán acceder a los sistemas de información utilizando una cuenta de usuario y una contraseña válida en la red.
- El responsable de cada proceso mantendrá un esquema de clasificación de los activos de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, de acuerdo con los niveles de seguridad establecidos en cada una de los procesos, teniendo como base la información registrada en la gestión de activos de información, los cuales se encuentran en el formato de inventario de activos en el repositorio organizacional.
- El responsable de TI controla el software y los equipos autorizados que podrán ser utilizados por los usuarios de la red de datos de la entidad para la creación, edición y desarrollo de nuevos activos de información.
- El responsable de TI dispondrá de respaldos y será el encargado del restablecimiento de los programas que han sido adquiridos en los equipos asignados a cada uno de los empleados para el desempeño de sus actividades. El uso de programas sin su respectiva licencia y sin la autorización, obtenidos a partir de otras fuentes, puede implicar amenazas

legales y de seguridad de la información para la entidad, por lo que esta práctica no está autorizada.

- Ningún usuario de la red de datos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO podrá copiar información clasificada o reservada sin la debida autorización.
- No se podrá utilizar la información de la entidad para otros fines; el usuario que infrinja esta norma será sancionado ya sea por copiar la información, sustraerla o causar algún daño sea intencional o no.
- Ningún equipo de cómputo presentará obsolescencia o daño irreparable, si esto pasa se tendrán los lineamientos correspondientes y necesarios para dar de baja el software y el equipo.
- Los activos de información pertenecen a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

- Las computadoras personales no se deben utilizar en los hogares para conectarse a Internet u otras redes si no existen controles para los virus y firewall de la computadora personal, instalados y en constante funcionamiento.
- Durante los viajes, los equipos (y medios) no se deben dejar desatendidos en lugares públicos. Las computadoras portátiles se deben llevar como equipaje de mano.
- Los portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les deben proporcionar una forma apropiada de protección al acceso (ej. Contraseñas de encendido, inscripción, etc.) Con el fin de prevenir acceso no autorizado.
- Proteger los equipos contra la exposición de campos electromagnéticos muy fuertes.
- Los equipos de cómputo y dispositivos móviles de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, así como la información almacenada en los mismos, son propiedad de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, y pueden ser inspeccionados, o utilizados de cualquier manera y en cualquier momento en que la entidad lo considere. Estos deben ser devueltos a la entidad en el momento en que el usuario deje de tener relación laboral con la entidad.
- Un computador personal equipo portátil, teléfono inteligente o cualquier otro sistema de cómputo usado para actividades de la entidad que contenga información sensible, no se deberá prestar a nadie y será responsabilidad exclusiva del funcionario que lo tenga asignado.
- Aceptar las configuraciones de seguridad del dispositivo por medio de correo electrónico, y estas no podrán modificarse mientras se acceda o almacene información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Instalar y configurar un software de antivirus.

- Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.
- Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.
- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
- Es necesario realizar el cifrado del dispositivo móvil.
- Está prohibido almacenar información personal en los dispositivos móviles asignados por TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.
- Está prohibido realizar instalación de aplicaciones no autorizadas por el área técnica.
- Está prohibido hacer volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.
- Configurar sólo las cuentas organizacionales en los dispositivos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO que tendrán acceso a la información de la Entidad.
- Para aquellos dispositivos que no son entregados por TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, deben recibir correo de la persona que envió solicitud a área técnica "**aceptando el cumplimiento la política de uso de activos de información, así como las configuraciones de seguridad establecidas"**.
- En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, se debe reportar la perdida al área técnica lo más pronto posible.
- En cualquier momento el equipo de Seguridad de la Información de la TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.
- Las Auditorías internas o de tercera parte pueden realizar la verificación de las configuraciones de los equipos móviles y su cumplimiento con los lineamientos de esta política.

RESPONSABILIDAD: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADO CLAVE: Dar cumplimiento a la política de uso de los activos de información

5.14 POLÍTICA DE USO DE DISPOSITIVOS DE ALMACENAMIENTO Y TRANSFERENCIA DE INFORMACIÓN

RESUMEN: Esta política establece los lineamientos para el correcto uso de dispositivos de almacenamiento extraíbles (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.), los cuales permiten una transferencia rápida y directa de la información. Se debe aplicar las medidas de seguridad que este tipo de dispositivos requieren por su susceptibilidad al robo, manipulación, extravío e infección por virus

Si se necesita almacenar información sensible o confidencial se utilizarán dispositivos externos corporativos debidamente protegidos, se almacenarán en lugares seguros y se informará al responsable si ocurre algún incidente (robo, pérdida, infección del dispositivo, etc.).

INTRODUCCIÓN: Para el cumplimiento de sus obligaciones TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO intercambia información entre funcionarios, contratistas, terceros y diferentes entes y por diferentes medios, por ello es necesario establecer unos lineamientos que garanticen que el intercambio de dicha información se realiza bajo los niveles de protección adecuados siempre que se vaya a transferir información personal, información pública clasificada o pública reservada.

Los medios de almacenamiento extraíbles permiten transportar y respaldar información de manera más fácil. Para asegurar la información contenida en los dispositivos extraíbles se deben aplicar medidas de seguridad que este tipo de dispositivos requieren, así como concientizar a los empleados y contratistas para su buen uso.

ALCANCE: Esta política es aplicable a funcionarios, contratistas y terceros que hagan uso de los dispositivos de almacenamiento de información pertenecientes a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer normas de uso de los dispositivos de almacenamiento que garanticen la seguridad de la información institucional en el intercambio de la misma entre funcionarios, contratistas y terceros de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIO

El responsable del dispositivo de almacenamiento extraíble deberá velar por el buen uso de la información restringida almacenada en el mismo, su adecuado control y distribución limitada. También deberá usar mecanismos de protección como el uso de contraseñas y/o encriptación de archivos.

El responsable del dispositivo de almacenamiento extraíble, deberá adoptar las medidas que se encuentren a su alcance para asegurar que los archivos contenidos en él se encuentren libres de virus, software y/o código malicioso que pueda poner en riesgo la confidencialidad, integridad y disponibilidad de la información y los equipos informáticos de la entidad.

Solo se puede realizar intercambio de información de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO entre su personal cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus labores.

Siempre que se realice intercambio de información catalogada como pública clasificada o pública reservada, dicho intercambio debe ser aprobado por el jefe directo o supervisor de contrato.

Todo intercambio de información electrónica perteneciente a TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO con terceros, debe ser respaldado con un acuerdo (convenio o contrato), incluyendo una cláusula de confidencialidad y no divulgación de la información proporcionada.

La solicitud de intercambio de información puede ser por requerimientos de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO del organismo externo o incluso de un tercero que, ante disposiciones legales o directrices del gobierno hacen necesaria dicha interoperabilidad.

La excepción en la entrega de información debe estar regida por lo establecido según legislación vigente.

La información recibida de otra entidad en Colombia se debe salvaguardar a un nivel igual o mayor que el aplicado por la entidad que originó el documento.

El intercambio de información digital pública clasificada y pública reservada, debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y que cumpla con la política de controles criptográficos, esto debe quedar registrado en los convenios o acuerdos de intercambio de información que firmen las partes.

El intercambio de información que se encuentre en formatos físicos debe estar debidamente etiquetada, en caso de que sea catalogada como pública clasificada o pública reservada, el intercambio debe realizarse en un sobre sellado para ser enviada a terceros.

Para el transporte de medios físicos de información sensible, se debe generar una bitácora de entrega de estos medios y recepción de estos.

Se debe transportar en un dispositivo con un sello de seguridad que garantice que en su desplazamiento no ha sido intervenido por un tercero.

Para la apertura de ese sello se debe generar un registro y garantizar que no se reutilice el sello.

Se deben transportar estos medios en un recipiente que proteja al activo de amenazas ambientales.

Toda información enviada desde TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO a través de correos electrónicos deberá incluir en su pie de página la siguiente advertencia:

"Este mensaje y cualquier archivo que se adjunte al mismo es confidencial y podría contener información clasificada y reservada de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, para el uso exclusivo de su destinatario. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo al remitente y borrar el mensaje recibido inmediatamente".

RESPONSABILIDAD: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO

RESULTADO CLAVE: Dar cumplimiento a la política de uso de dispositivos de almacenamiento.

5.15 POLÍTICA DE CONTROL DE ACCESO Y USO DE PUNTOS DE RED Y RED DE AREA LOCAL

RESUMEN: La presente política establece los parámetros necesarios para uso de puntos de red y el acceso adecuado a la red de área local de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO, con el fin de preservar la disponibilidad, confidencialidad e integridad de la información.

INTRODUCCIÓN: Los equipos suelen formar parte de una **red** de equipos. Una red permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Las redes de equipos crean un entorno informático potente y sofisticado. Sin embargo, las redes complican la seguridad de los equipos, debido a esto la política

de control de acceso de las redes logra impedir el acceso no autorizado a los servicios en la red. El acceso a la red es el primer aspecto que se debe tener en cuenta una vez instalado el software de red, garantizando que cada funcionario o contratista tenga acceso al servicio.

Una red de área local permite que los dispositivos se conecten, transmitan y reciban información entre ellos, utilizando herramientas de seguridad que permitan la protección de los mismos.

ALCANCE: Esta política es aplicada a funcionarios y contratistas que hacen uso de puntos de red y tienen acceso a la red de área local de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

OBJETIVO: Establecer lineamientos que permitan un correcto uso y acceso a puntos de red, así como el uso de la red de área local de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

PRINCIPIO

- Impedir el acceso no autorizado a los servicios de la red.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se ingrese a la red por medio de computación móvil e instalaciones de trabajo remoto.
- Se deberían controlar los accesos a servicios internos y externos conectados en red.
- Vigilar que los mecanismos de autenticación adecuados si se aplican a los usuarios y equipos.
- Los usuarios deben usar las redes LAN de la entidad de manera ética, razonable, responsable, no abusiva y sin afectar la disponibilidad, confidencialidad o integridad de la información de la entidad.
- A la red LAN de la entidad solamente deben conectarse los computadores de la entidad y su uso debe ser exclusivamente para fines laborales.
- Los usuarios no deben conectar a la red LAN dispositivos de red no pertenecientes a la entidad, como routers, módems, switchs, repetidores o access points, entre otros.
- Puerto de la red LAN que no esté en uso debe apagarse.

RESPONSABILIDAD: funcionarios y contratistas de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO.

RESULTADO CLAVE: Dar cumplimiento a la política de control de acceso a redes.

6. PROCEDIMIENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD

Los procedimientos son uno de los elementos dentro de la documentación del Manual de políticas de Seguridad de la Información. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él, se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

También es recomendable el uso de instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y operación; los primeros para la ejecución de las tareas por la persona y los segundos para la manipulación o la operación de un equipo.

Los usuarios de TELEVISIÓN REGIONAL DEL ORIENTE LTDA. CANAL TRO pueden consultar las descripciones detalladas de cada procedimiento a través del Sistema Integrado de Gestión SIG.

6.1 PROCEDIMIENTO DE CONTROL DE DOCUMENTOS

Garantiza que la entidad cuente con los documentos estrictamente necesarios a partir de su perfil de actuación en cada momento y maneja la dinámica del mejoramiento, mostrando la realidad que atraviesa la entidad en cada momento, porque incorpora la eficacia de las diferentes acciones, a través de la revisión documental y del cumplimiento de los requisitos idénticos en los diferentes modelos de gestión sobre el control de documentos. Así mismo, busca garantizar que los documentos en uso, sean confiables y se mantengan actualizados, una vez se evidencie la eficacia de las acciones correctivas, preventivas y de mejora que hacen que los procesos se ajusten y evolucionen; de igual manera que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implementó como solución a un problema, riesgo o a una oportunidad se conserven.

De acuerdo a la correspondencia y vínculos técnicos de la norma ISO 9001:2015 se utiliza: **Procedimiento para el Control de los Documentos V-GM-P01, Guía para la Producción de Documentos A-GD-P01** del Sistema Integrado de Gestión SIG.

6.2 PROCEDIMIENTO DEL CONTROL DE REGISTROS

Está definido para evidenciar las acciones realizadas y los resultados obtenidos en la ejecución de las actividades, con el fin de analizar los datos, y lo que es más importante, para la toma de decisiones, de tal forma que registro que no aporta valor o no lleva a una decisión de mejora o de acción, no se debe tener en el sistema, ya que lo único que haría es desgastar a la entidad y generar residuos sólidos como papel mal utilizado.

De acuerdo a la correspondencia y vínculos técnicos de la norma ISO 9001:2015 se utiliza el **Procedimiento de Control de Registros A-GD-P03** del Sistema Integrado de Gestión - SIG.

6.3 PROCEDIMIENTO DE AUDITORÍA INTERNA

La auditoría interna es una herramienta para la Alta Dirección, en el momento de determinar la eficacia y la eficiencia del sistema de gestión, a través de la identificación de las fortalezas y debilidades. Esta es la razón por la cual se recomienda siempre realizar auditorías internas antes de llevar a cabo la revisión gerencial, ya que para esta última se requiere información sobre el sistema y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema de gestión.

Se hacen auditorías para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación del sistema de gestión, para evaluar el estado de mantenimiento y la capacidad de mejoramiento del sistema de gestión.

De acuerdo a la correspondencia y vínculos técnicos de la norma ISO 9001:2015 se utiliza el **Procedimiento Evaluación y Seguimiento al Sistema de Gestión de Calidad - SGC y al Sistema de Control Interno – SCI V-GE-P01** del Sistema Integrado de Gestión.

6.4 PROCEDIMIENTO DE ACCIÓN CORRECTIVA

El objetivo de este procedimiento es definir los lineamientos para eliminar la causa de no conformidades asociadas con los requisitos de la política de seguridad de Televisión Regional del Oriente Ltda. Canal TRO, así como: definir los lineamientos

para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

De acuerdo a la correspondencia y vínculos técnicos de la norma ISO 9001:2015 se utiliza el **Procedimiento de Acciones Correctivas y/o de Mejora y Procedimiento de Acciones de Mejora Continua V-GM-P05.**

6.5 PROCEDIMIENTO DE ACCIÓN PREVENTIVA

El objetivo de este procedimiento es definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real y eliminar sus causas.

De acuerdo a la correspondencia y vínculos técnicos de la norma ISO 9001:2015 se utiliza el **Procedimiento de Acciones Correctivas y/o de Mejora y Procedimiento de Acciones de Mejora Continua V-GM-P05.**

7. PROCESO DISCIPLINARIO

El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y otros colaboradores de Televisión Regional del Oriente Ltda. Canal TRO violen las políticas y los procedimientos de seguridad de la información, así como cualquier otra violación de la seguridad.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por Televisión Regional del Oriente Ltda. Canal TRO:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo al área técnica, equipo de incidentes de seguridad de la información.
- No mantener la confidencialidad de las contraseñas de acceso a las redes sociales y cuentas de correo electrónico asociadas a las mismas, o permitir que otras personas accedan con el usuario y clave del titular.

- Permitir el acceso u otorgar privilegios de acceso a las redes sociales a personas no autorizadas.
- Ejecución de cualquier acción que conlleve a la difamación, que llegue afectar la reputación o presentar una mala imagen de Televisión Regional del Oriente Ltda. Canal TRO.
- Eliminar documentos de las Tablas de Retención Documental sin la debida justificación o enviar intencionalmente a un destinatario que no corresponde a las comunicaciones recibidas en la entidad.
- Ocasionar daño o dar lugar a la pérdida de expedientes, documentos o archivos que hayan llegado a su poder por razón de sus funciones/actividades.
- Dar lugar a la pérdida de expedientes, documentos, información o archivos a personas no autorizadas.
- Realizar actividades tales como borrar, alterar o eliminar información de manera malintencionada. Sustraer de las instalaciones de Televisión Regional del Oriente Ltda. Canal TRO, documentos de archivo sin la debida autorización.
- No hacer entrega de los documentos de archivo que se encuentran a cargo de los funcionarios y contratistas, debidamente inventariados, cuando se presente su retiro o traslado.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Calificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, *“documentos impresos que contengan información pública reservada, información pública clasificada”.*
- No guardar la información digital, producto del procesamiento de la información perteneciente a Televisión Regional del Oriente Ltda. Canal TRO.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios.
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a Televisión Regional del Oriente Ltda. Canal TRO, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.

- Solicitar cambios de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la entidad, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferente a los asignados por la entidad.
- Enviar información pública reservada y/o información pública clasificada, por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar los equipos electrónicos o tecnológicos desatendidos o que, a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el área técnica de Televisión Regional del Oriente Ltda. Canal TRO.
- Permitir el acceso de funcionarios y/o contratistas a la red corporativa, sin la autorización del área técnica de Televisión Regional del Oriente Ltda. Canal TRO.
- Utilización de servicios disponibles a través de internet, como FTP, no permitidos Televisión Regional del Oriente Ltda. Canal TRO o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de Televisión Regional del Oriente Ltda. Canal TRO.
- No cumplir con las actividades designadas para la protección de los activos de información de Televisión Regional del Oriente Ltda. Canal TRO.
- Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no pertenezca a Televisión Regional del Oriente Ltda. Canal TRO o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de Televisión Regional del Oriente Ltda. Canal TRO, sin la debida autorización.

- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de Televisión Regional del Oriente Ltda. Canal TRO para beneficio personal.
- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo o en contra de la voluntad del Televisión Regional del Oriente Ltda. Canal TRO.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones del Televisión Regional del Oriente Ltda. Canal TRO, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información del Televisión Regional del Oriente Ltda. Canal TRO.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica del Televisión Regional del Oriente Ltda. Canal TRO.
- El que viole datos personales de las bases de datos del Televisión Regional del Oriente Ltda. Canal TRO.
- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por el Televisión Regional del Oriente Ltda. Canal TRO.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de Televisión Regional del Oriente Ltda. Canal TRO o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de Televisión Regional del Oriente Ltda. Canal TRO a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de Televisión Regional del Oriente Ltda. Canal TRO o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por Televisión Regional del Oriente Ltda. Canal TRO.
- Retirar de las instalaciones de la entidad, estaciones de trabajo o computadores portátiles que contengan información institucional sin las autorizaciones pertinentes.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.

- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de Televisión Regional del Oriente Ltda. Canal TRO, para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de Televisión Regional del Oriente Ltda. Canal TRO o de alguno de sus funcionarios.
- Realizar cambios no autorizados en la plataforma tecnológica de Televisión Regional del Oriente Ltda. Canal TRO.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el área técnica de Televisión Regional del Oriente Ltda. Canal TRO.
- Copiar sin autorización los programas de Televisión Regional del Oriente Ltda. Canal TRO, o violar los derechos de autor o acuerdos de licenciamiento.

8. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la entidad, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando n impacto mínimo o nulo ante una contingencia.

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI de Televisión Regional del Oriente Ltda. Canal TRO podrán ser restaurados dentro de escalas de tiempo razonables.

Televisión Regional del Oriente Ltda. Canal TRO deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI de Televisión Regional del Oriente Ltda. Canal TRO de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
- Documentación de la estrategia del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

La continuidad del negocio deberá ser gestionada por la Gerencia de Televisión Regional del Oriente Ltda. Canal TRO.

La Alta Dirección de Televisión Regional del Oriente Ltda. Canal TRO será la responsable de velar por la implantación de las medidas relativas a ésta. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

9. CUMPLIMIENTO

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de Televisión Regional del Oriente Ltda. Canal TRO. En caso de que violen las políticas de seguridad ya sea de forma intencional o por negligencia, Televisión Regional del Oriente Ltda. Canal TRO tomará las acciones disciplinarias y legales correspondientes.

El Manual de Políticas de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

10. CONTROLES

El Manual de Políticas de Seguridad de la Información de Televisión Regional del Oriente Ltda. Canal TRO está soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual.

11. MARCO LEGAL

- Constitución Política de Colombia 1991. Reconoce como Derecho Fundamental el Habeas Data.
- Artículo 20. Libertad de Información.
- Código Penal Colombiano – Decreto 599 de 2000.
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por el cual se dictan Normas para el ejercicio de control interno MECI para el Estado Colombiano.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual – Derechos de Autor.
- Ley 594 de 2000 – Ley General de Archivo.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.

- Ley 527 de 1999, por 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.
- Directiva Presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en Línea.
- Ley 1266 de 2008, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en Bases de Datos Personales.
- Ley 1273 de 2009, “Delitos Informáticos” protección de la información y los Datos.
- Ley 1437 de 2011, “Código de procedimiento administrativo y de lo contencioso administrativo”.
- Ley 1581 de 2012, “Protección de Datos Personales”.
- Decreto 2609 de 2012, por la cual se reglamenta la Ley 594 de 2000 y Ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la Ley 1581 de 2012.
- Ley 1712 de 2014, “De Transparencia y del derecho de acceso a la información pública nacional”.
- Ley 962 de 2005. “Simplificación y Racionalización de Trámites. Atributos de seguridad en la Información electrónica de entidades públicas”.
- Ley 1150 de 2007. “Seguridad de la Información electrónica en Contratación en Línea”.
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de Seguridad”.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad Digital.

12. RESPONSABLE DEL DOCUMENTO

Líder de Área Técnica y Emisión.

13. CONTROL DE CAMBIOS

Versión	Descripción del cambio	Fecha
01	Versión inicial del manual	Noviembre 18 de 2021

Elaboró	Aprobó
Líder del proceso de Gestión Técnica	Comité de Gestión y desempeño Institucional