Políticas de Seguridad de la Información

Teveandina S.A.S. – Canal Trece

Revisiones y control de cambios

Titulo	**Políticas de Seguridad de la Información, TEVEANDINA S.A.S. – CANAL TRECE**
Autores	Camilo Andres Beltrán, Wilmar López
Tema	Políticas de Seguridad de la Información
Fecha de Elaboración	Marzo 2024
Formato	PDF
Versión	2.0
Palabras Relacionadas	MSPI, gestión de riesgos, políticas de seguridad de la información

Control de Cambios			
Fecha	**Autores**	**Versión**	**Cambio**
Marzo 2024	Camilo Beltrán Wilmar López	2.0	Este documento Contempla V1.2 con fecha Marzo 2023, se realizó actualización de formato y de codificación, adicionalmente se actualizó el contenido de la política en cumplimiento de la normatividad vigente.

TABLA DE CONTENIDO

1. DEFINICIONES

INFORMACIÓN: Hace referencia al conjunto de datos organizados para la trasmisión de un mensaje en un contexto específico con el fin de incrementar el conocimiento

TECNOLOGÍA DE INFORMACIÓN: Conjunto de tecnologías que permiten administrar el uso de los datos de una manera funcional

SISTEMA DE INFORMACIÓN: El sistema de información es un conjunto de elementos, los cuales se encuentran dispuestos para el tratamiento y administración de los datos o información.

SEGURIDAD DE LA INFORMACIÓN: La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, rentabilidad, cumplimiento legal e imagen institucional.

MSPI: Hace referencia a el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información.

INTEGRIDAD: Mantenimiento sobre la exactitud y completitud en la información.

DISPONIBILIDAD: Acceso y uso de la información bajo los sistemas que la procesan y mantienen por parte de los procesos que la requieran.

CONFIDENCIALIDAD. Hace referencia a prevenir la divulgación no autorizada de la información.

INFORMACIÓN: Es un conjunto organizado de datos procesados los cuales conforman un mensaje, recibido y procesado por sistemas o herramientas informáticas.

DATO: Es una representación simbólica la cual puede ser numérica, alfabética, algorítmica, espacial, sobre un atributo o variable.

COPIAS DE SEGURIDAD: Se refiere a la copia de los datos originales en un medio magnético que permitan ser recuperadas en caso de pérdida.

SERVIDOR: Es un dispositivo que integra hardware y software para recibir y atender peticiones de clientes, con el fin de entregarle una respuesta conforme.

ACTIVO DE INFORMACIÓN: Hace referencia a todo aquello que es considerado importante y con alto valor debido a que puede contener información relacionada con bases de datos, contraseñas, entre otros.

RIESGO: Posibilidad que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

VULNERABILIDAD: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

2. OBJETIVOS DE LA POLÍTICA

Son objetivos de la política:

- Proteger los recursos de la Entidad ante posibles riesgos y amenazas internas y externas, con el fin de mantener la integridad, confidencialidad y disponibilidad sobre la información.
- Implementar controles sobre todos los procesos que hacen uso de sistemas, servicios y herramientas informáticas relacionados con su debido uso.
- Garantizar la actualización periódica de la política como medio para la protección de los activos de información ante nuevas amenazas.
- Definir y socializar las políticas y lineamientos necesarios para asegurar la protección de la información y asegurar el cumplimiento de la integridad, disponibilidad y confidencialidad y el no repudio de dicha información.
- Divulgar y cumplir las políticas referidas en el presente documento, ejecutando mantenimientos, actualizaciones y mejoras que sean pertinentes, para garantizar la mejora continua de procesos, controles y dominios, mitigando riesgos desde cualquier flanco de Seguridad.

3. ALCANCE

La Política de seguridad de la información vigente y expedida por EL CANAL REGIONAL DE TELEVISIÓN TEVEANDINA S.A.S - CANAL TRECE de apreciación Informativo y carácter obligatorio para todos los usuarios del canal. Incluye la creación, objetivos, alcances y objetivos a políticas de seguridad involucrando a todos funcionarios, contratistas y terceros que realicen trabajo en la entidad. El alcance se extiende desde la declaración de la directiva del presente documento, las directrices para la implantación de sistemas de seguridad y protección de datos, en la definición de información, matrices de riesgo e indicadores de seguimiento, enfocados en el cumplimiento de políticas hasta la definición de estrategias de implementación

4. MARCO REGULATORIO Y NORMATIVO

EL CANAL REGIONAL DE TELEVISIÓN TEVEANDINA S.A.S - CANAL TRECE como entidad pública tiene en cuenta las siguientes disposiciones legales y marcos de referencia para el desarrollo de Modelo de Seguridad y Privacidad de la Información (MSPI) dentro del marco de la implementación de la política de Gobierno Digital.

- Ley 1712 de 2014
- Ley 1581 de 2012.
- Decreto 2693 de 2012
- Decreto 1008 de 2018
- Decreto 415 de 2016 MinTic
- NTC-ISOIIEC 27001- 27002:2023
- Ley 734 de 2022 "Por la cual se expide el código disciplinario único"
- Según la Norma Ley 1952 2019 por medio de la cual se explique el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.

5. PROCESO DISCIPLINARIO

Dentro de la estrategia de la seguridad de la información, EL CANAL REGIONAL DE TELEVISIÓN TEVEANDINA S.A.S - CANAL TRECE seguirá el proceso establecido de la ley 734 de 2002 y la ley 1952 de 2019, para investigar a los trabajadores oficiales que hayan infringido y violentado a la presente ley. El proceso disciplinario también se debe utilizara como medida preventiva para evitar que los trabadores oficiales, contratistas y los otros colaboradores, transgredan las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad sin justificación alguna. El adelantamiento de los procesos disciplinarios corresponde a la Dirección de Control Disciplinario Interno y de la Procuraduría General de la Nación, de acuerdo con las competencias señaladas en la ley. Actuaciones que conllevan a la violación de la seguridad de la información en Teveandina S.A.S.,

No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello, será interpretado como coacción de hecho, y podrá ser tratado judicial y penalmente cual sea el caso.

6. DESCRIPCIÓN DE LA POLÍTICA

6.1 Generalidades

Esta política recoge los siguientes aspectos que incluyen normas sobre:

- Uso de los activos de información
- Uso de los sistemas de información y servicios tecnológicos
- Cuentas de usuario y contraseñas
- Uso de redes alámbricas e inalámbricas
- Uso de dispositivos de almacenamiento
- Condiciones del centro de cómputo y datos
- Copias de seguridad
- Escritorios y pantallas limpias

6.2 Sanciones Por Incumplimiento A La Política

Es obligación de todos los colaboradores de la Entidad salvaguardar la información a partir de las funciones asignadas, por cuanto el incumplimiento de esta política tendrá sanciones de tipo administrativo y legal, condicionadas por la gravedad de los aspectos infringidos, previa evaluación del equipo de seguridad de la información (ESI).

la necesidad de clasificar las violaciones de la política de seguridad de la información es tomar medidas correctivas de acuerdo con la clasificación y niveles de mitigación establecidos Impacto potencial en la seguridad de la información. Se puede considerar la acción correctiva Desde actuaciones administrativas hasta procesos disciplinarios o penales, si las condiciones son las adecuadas.

No obstante, se debe determinar y aprobar sanciones por incumplimiento de las políticas de seguridad de la información. Para garantizar el pleno cumplimiento de esta política de seguridad y mejorar La información utilizada en los procesos transversales de la organización, será el beneficio más importante de la información, Así, la capacidad de brindar información oportuna y verificable para la toma de decisiones

7. ESTRUCTURA SEGURIDAD DE LA INFORMACIÓN (ESI)

7.1 Objetivo

Establecer las políticas de seguridad aplicables a nivel administrativo, técnico y de seguridad. incluyendo una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo con su estructura organizacional.

7.2 Alcance

Establecer un esquema corporativo y de carácter empresarial, que deberá cumplir determinadas aplicabilidades dentro Teveandina S.A.S. Canal Trece, con el fin de mantener y salvaguardar la información que se maneja dentro y fuera del canal. Teniendo como importancia el cumplimiento de la presente política sin excepción alguna

7.3 Responsabilidades

Esta política bajo su literal 7.7 y definiendo a detalle las responsabilidades de quien establezca los compromisos, será dentro y fuera de Teveandina S.A.S.– Canal Trece el encargado acatar y mantener gestión del presente documento.

7.4 Generalidades

Esquema de seguridad Información mediante la definición y establecimiento de roles y responsabilidades Actividades de operación, gestión y aseguramiento de la seguridad de la información Establecimiento del Comité de Seguridad de la Información, etc.

7.5 Política Estructural y organizacional de Seguridad de la Información

Crear un esquema de seguridad definiendo y estableciendo roles y responsabilidades, que integren actividades de operación, gestión y gobierno de la seguridad de la información establecimiento el Comité de Seguridad de la Información. Las políticas de seguridad de la información deben validarse, definirse, implementarse y revisarse mediante actualización para proteger los activos de la entidad.

Las Consultas, solicitudes y compras de productos y servicios de equipos TI, el desarrollo y la adquisición de software se revisan, validan y gestiona por el Departamento de Tecnologías de la Información y las Comunicaciones, respecto al software, debe cumplir con los requisitos y obligaciones derivados del presente documento y sus políticas, y cumplir Sobre la Ley de Propiedad Intelectual y la Ley de Derechos de Autor.

7.6 Política de Comité de Seguridad de la información

El comité de seguridad estará conformado por:

- Gerente
- Líder Administrativo y Financiero.
- Líder de Planeación
- Líder y/o CIO TI
- Director jurídico y administrativo
- Líder de Comunicaciones
- CISO y/o Personal encargado seguridad de la información
- Líder Control Interno
- Personal encargado de la infraestructura y las comunicaciones
- Equipo de Arquitectura y Gobierno Digital

Funciones del Comité de Seguridad de la Información:

El Comité de seguridad de la información, en su papel de guía para la implementación de la estrategia de Gobierno Digital según el artículo 2.2.9.1.1.1 del Decreto 1078 de 2015, debe:

- Proponer y verificar el cumplimiento de normas y políticas de seguridad, asegurando acciones preventivas y correctivas para proteger equipos, instalaciones de cómputo, bases de datos y la información en general.
- Revisar el estado general de la seguridad de la información.
- Analizar y revisar los incidentes de seguridad de la información existentes.
- Aprobar y revisar los proyectos relacionados con la seguridad de la información.
- Formular nuevas políticas de seguridad de la información o modificar las existentes.
- Colaborar en la creación y evaluación de planes de acción para mitigar o eliminar riesgos.
- Identificar la necesidad de evaluar los procesos que dependen de los recursos informáticos y su infraestructura tecnológica.
- Realizar otras actividades inherentes al comité relacionadas con la seguridad de la información.
- Fomentar la mejora continua del Sistema de Gestión de Seguridad de la Información.

Las funciones del Comité de Seguridad de la Información estarán alineadas con las desarrolladas por MINTIC, el cual es responsable de aprobar las modificaciones o nuevas políticas de seguridad de la información y orientar la implementación de la estrategia de Gobierno Digital.

Funciones del secretario técnico:

- Convocar a los integrantes del Comité a las sesiones ordinarias y extraordinarias.
- Enviar la agenda a los miembros del Comité con tres días de antelación.
- Verificar el quórum al inicio de las sesiones.
- Recibir y preparar respuestas a los documentos que sean competencia del Comité.
- Firmar las actas que hayan sido aprobadas.
- Dar seguimiento a los compromisos y tareas pendientes del Comité.
- Elaborar las actas de reunión del Comité de manera oportuna.
- Mantener y custodiar el archivo de las actas y demás documentos del Comité.
- Realizar otras tareas que le sean asignadas por el Comité.

Responsabilidades del Comité de Seguridad de la Información:

Los integrantes del Comité de Seguridad de la Información son responsables de:

- Analizar, revisar y centralizar todas las acciones relacionadas con la gestión de la seguridad de la información en la organización, manteniendo actualizadas las políticas según las necesidades y requerimientos de Teveandina S.A.S.– Canal Trece.
- Garantizar el apoyo y dirección gerencial en cuanto a los principios y metas para administrar y desarrollar iniciativas de seguridad de los activos de información, asegurando el compromiso adecuado y los recursos necesarios para formular y mantener políticas de seguridad de la información a través de todos los niveles de la organización.
- Validar las políticas y procedimientos de seguridad de la información para el uso adecuado y la administración de los recursos informáticos asignados a los servidores públicos y contratistas, garantizando la protección de la información.
- Establecer directrices para el uso y manejo de dispositivos móviles *7.8 POLITICA DE DISPOSITIVOS MÓVILES* (teléfonos móviles, smartphones, tabletas, entre otros) proporcionados por Teveandina S.A.S.– Canal Trece.
- Definir la estrategia informática para alcanzar los objetivos y minimizar los riesgos institucionales.
- Monitorear el estado de los proyectos en términos de calidad de los productos, tiempo y costos.
- Seguir y verificar la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información (SGSI).
- Asegurar la aprobación de presupuestos para las actividades del SGSI.

Equipo de respuesta a incidentes:

Para facilitar la implementación, seguimiento y mejora continua, se define el equipo de respuesta a incidentes o CSIRT (Computer Security Incident Response) Teveandina S.A.S.– Canal Trece, el cual estará compuesto por:

- Líder y/o CIO TI Profesionales especializado.
- CISO o Consultores especialistas en seguridad de la información.
- Comité de Seguridad de la información.

La definición de roles y responsabilidades específicas se detalla en un documento independiente, ajustado a las condiciones del manual de funciones de Teveandina S.A.S.– Canal Trece y con aprobación del Comité.

Funciones del equipo de respuesta a incidentes o CSIRT:

- Registrar detalladamente y comunicar por escrito de manera oportuna la ocurrencia de eventos e incidentes de seguridad de la información, para que el área de TI y, en casos mayores, el Comité de Seguridad de la Información, tomen las acciones pertinentes.
- Coordinar con el área de Tecnologías de la Información, la definición de proyectos y medidas de seguridad de la información.
- Presentar propuestas sobre información relacionada e indicadores para que el Comité de Seguridad de la Información determine su relevancia para Teveandina S.A.S.– Canal Trece.
- Proporcionar recomendaciones sobre las condiciones necesarias para asegurar la protección de la información.
- Asesorar y diseñar acciones para guiar, capacitar y mejorar la seguridad de la información en Teveandina S.A.S.– Canal Trece

7.7 Política de Funciones y Responsabilidades

El ESI tendrá las siguientes funciones:

- Supervisar la ejecución y cumplimiento de la política a partir de su aprobación y divulgación, con el fin de asegurar la información en todos los niveles.
- Vigilar cambios sobre riesgos a partir de nuevas amenazas y vulnerabilidades en la información a través de análisis periódicos al menos una vez al año.
- Controlar diferentes incidentes de seguridad sobre la información por medio de las normas establecidas en esta política de seguridad.
- Promover la difusión de la política de seguridad de información a todos los colaboradores de la Entidad a través de planes de capacitación y apropiación.

7.8 Política de dispositivos Móviles

- Se debe llevar un registro y control de todos los dispositivos móviles propiedad de la entidad.
- Los dispositivos móviles utilizados para realizar tareas profesionales deben usarse con prudencia.
- Debe definirse un procedimiento formal de salida.
- Los dispositivos móviles deben protegerse mediante el uso y la implementación de controles apropiados, tales como; Cifrar la información, restringir políticas para ejecutar aplicaciones y conexiones de dispositivos USB, deshabilitar el acceso inalámbrico cuando se conecta a una red LAN, etc.
- Todos los dispositivos móviles, como los teléfonos móviles que almacenan información, requieren un sistema de autenticación, como un patrón, un código de desbloqueo o una contraseña.

- Cualquier funcionario, contratista, tercero o aprendiz responsable de un dispositivo móvil, debe realizar copias de seguridad periódicas. al menos una vez por semana para ejecutar una copia de seguridad de la carpeta dedicada a esta función.
- Todos los empleados y terceros son responsables del uso adecuado de los dispositivos móviles en redes seguras y de garantizar las protecciones adecuadas para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada en los mismos

7.9 Política de Trabajo en Casa o Teletrabajo

El teletrabajo debe ser aprobado y reglamentado por la Oficina de Talento Humano. Basados sobre la Ley N° 1221 de 2008: "Por la cual se establecen Normas para la Promoción y Regulación del Teletrabajo" y Decreto N° 884 de 2012: "De acuerdo con la Ley N° 1221 de 2008, Compromiso de Uso Correcto de la Información".

El teletrabajo sólo está permitido en casos de emergencia o especiales. Ley N° 2088 de 12 de mayo de 2021 "Reglamento sobre teletrabajo." Este debe estar aprobado por la gerencia de Teveandina Canal Trece y la Oficina de Talento Humano.

El acceso remoto a los recursos corporativos desde computadoras remotas o equipos tecnológicos (Celulares, Tablet, etc) debe ser a través de una conexión VPN proporcionada por el área de Tecnología de la información y las comunicaciones (TI). Sí, y solo sí se proporciona acceso a recursos establecidos bajo la política CID.

8. CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

8.1 Objetivo

Conservar, proteger la información generada por los diferentes procesos de la entidad, evitando pérdida de información por amenazas potenciales en el medio ambiente, ataques cibernéticos o Degradación de la Información

8.2 Alcance

Esta política aplica las buenas prácticas de identificación bajo datos básicos y de mayor complejidad, dando alcance a los inventarios de codificación y gestión. Para posterior ubicación en zonas, lugares, procesos item dentro de Teveandina S.A.S – Canal Trece

8.3 Responsabilidades

Establece que el oficial de seguridad y los lideres encargados de ellos, encabezan las buenas prácticas de identificación, valoración, clasificación y tratamiento de estos activos de información.

8.4 Generalidades

Con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información, se establecen los siguientes criterios para su control a partir de la siguiente clasificación dispuesta por la ley 1712 de 2014:

- Información pública
- Información pública clasificada
- Información pública reservada

8.5 Política Clasificación de la información

Es responsabilidad de la Entidad identificar y clasificar la información de acuerdo con los niveles establecidos, de tal forma que el proceso de gestión de tecnologías convergentes, gestión documental, la dirección jurídica y administrativa definen las directrices para la gestión y clasificación de los activos de información y sus medidas de tratamiento, tanto para los activos internos y externos.

8.6 Política Gestión y etiquetado de la información

Los colaboradores de la Entidad deben mantener organizado el archivo de gestión físico y digital de acuerdo con lo establecido por gestión documental, los líderes de proceso deben establecer mecanismos para el control de sus activos de información con el fin de mantener la disponibilidad, integridad y confidencialidad. La Entidad dispone de los medios físicos y tecnológicos para que los colaboradores realicen una gestión segura de la información.

9. GESTIÓN DE SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS

9.1 Objetivo

Proporcionar calidad donde se perciba el aumentando, la eficiencia, la identificación, el registro y control del inventario de los sistemas de información de Teveandina S.A.S – Canal Trece, alineando con procesos de negocio e infraestructura TI, reduciendo así, riesgos asociados a los servicios TI. Amparado bajo el conjunto de normas y estándares internacionales. Como el ISO/IEC 27001.2023. Adicionalmente

9.2 Alcance

Teveandina S.A.S – Canal Trece y la presente política, confía en los sistemas de información y tecnología para lograr una ventaja competitiva, alcanzando la excelencia operativa, con nuevos productos, servicios y modelos de negocio, acercamiento con clientes y proveedores y una toma de decisiones eficiente. La capacidad de utilizar la política está al alcance de la organización. Aprovechando el desarrollo de estas características le dará una ventaja sobre sus competidores.

9.3 Responsabilidades

La política establece tareas y funciones a los encargados de las áreas, con apoyo del oficial de seguridad, impulsando resultados en el sistema de información y nuevas tecnologías, donde se visualice el cumplimiento de objetivos y alcances propuestos. Los empleados en el área de tecnología, como actor principal de responsabilidad, no deben contar con conocimientos avanzado para poder cumplir con los resultados de la presente política y directrices impartidas en el presente documento.

9.4 Generalidades

Esta política hace referencia a normas concernientes para el manejo de los servicios tecnológicos y sistemas de información en operación

9.5 Política de Identificación y Registro de sistemas de información

- Se deben identificar todos los sistemas de información utilizadas en el entorno
- Los propietarios de sistemas de información deben mantener un registro actualizado de todas las aplicaciones bajo su responsabilidad, incluyendo información relevante

como el nombre de la aplicación, la descripción, la versión, el propósito, la ubicación de los datos, los usuarios autorizados y cualquier riesgo de seguridad asociado.
- Se debe realizar una evaluación de riesgos para cada sistema de información con el fin de determinar su nivel de criticidad y los controles de seguridad requeridos.

9.6 Política de Control de Inventario, Retiro y/o Desinstalación

- El inventario de sistemas de información debe estar centralizado y accesible a los responsables de seguridad de la información y aprobado por la alta dirección.
- El inventario debe mantenerse actualizado en tiempo real y revisarse periódicamente para garantizar su precisión.
- Se deben establecer procedimientos de gestión de cambios para las aplicaciones, asegurando que cualquier cambio en la configuración o en el estado de una aplicación se registre y se evalúe desde una perspectiva de seguridad.
- Cuando un sistema de información ya no sea necesaria o segura para su uso, se debe seguir un procedimiento de retiro adecuado que incluya la eliminación segura de datos y la documentación del proceso.
- Se deben revisar y evaluar los sistemas de información obsoletas o en desuso de forma periódica y tomar medidas adecuadas para su desmantelamiento.
- Se realizarán auditorías periódicas para verificar el cumplimiento de esos sistemas de información.

9.7 Política Uso aceptable de los sistemas y herramientas de información

Todos los colaboradores de la Entidad deben hacer un uso adecuado de los sistemas de información y herramientas asignadas para su trabajo diario las cuales son asignadas por Teveandina – Canal Trece a través de los siguientes criterios:

Cada equipo de cómputo será entregado con el siguiente software básico para asegurar su funcionamiento (equipos propios y en alquiler)

- Sistema Operativo Windows o MacOS
- Office 365, incluye: Word, Excel, Power Point, Outlook (correo electrónico), Teams, SharePoint, One Drive (1TB de almacenamiento)
- 7-zip, WinRAR
- Firefox, Google Chrome
- Antivirus
- ERP SYSMAN (en los casos que aplique)
- ORFEO (En los casos que aplique)
- Software básico equipos de postproducción de acuerdo con las necesidades del proceso (Adobe CC, Códecs, entre otros)

La instalación de software es responsabilidad de los colaboradores de proceso de tecnologías convergentes, siendo los únicos autorizados para realizar esta actividad, atendiendo las solicitudes hechas por la herramienta de soporte a usuarios.

Si un colaborador tiene instalado aplicaciones diferentes a las mencionadas anteriormente, estas serán desinstaladas sin autorización. Esta consideración aplica para equipos propios y en alquiler.

Ningún colaborador debe realizar cambios en la configuración de los equipos, tales como como conexiones de red, papel tapiz corporativo, configuración BIOS, modificación de registros a través de REGEDIT e ingreso a consola. Estos cambios solo deben ser realizados por los colaboradores de proceso de tecnologías convergentes. Esta consideración aplica para equipos propios y en alquiler.

El proceso de tecnologías convergentes es la responsable de mantener la lista del software y aplicaciones permitidas por la Entidad para ser instaladas en los equipos de cómputo y dispositivos, así mismo deberá controlar el licenciamiento del software y aplicaciones.

Únicamente los colaboradores autorizados por el proceso de tecnologías convergentes podrán utilizar herramientas de gestión remota de acuerdo con los esquemas de seguridad brindados por la Entidad.

Todos los colaboradores de la Entidad son responsables por el buen uso de los servicios tecnológicos, herramientas y sistemas de información asignados, por cuanto no pueden ser usados en beneficio propio, para prácticas ilícitas o con mala intención que atenten con otros colaboradores, legislación vigente, lineamientos internos y demás establecidas.

La información personal almacenada en equipos de cómputo u otros dispositivos, debe ser guarda en una carpeta nombrada como PERSONAL.

Los equipos, dispositivos, periféricos herramientas y sistemas de información asignados deben ser entregados al finalizar el contrato o gestión de los colaboradores de Teveandina S.A.S – Canal Trece. Esto será desarrollado en conjunto con el proceso de almacén y archivo para efectos de hacer entrega de paz y salvo.

Todos los contratistas deben garantizar que la información correspondiente a su gestión sea entregada al supervisor a través del servicio en la nube o por un dispositivo de almacenamiento. Así mismo, cada colaborador debe ser responsable de sacar el respaldo respectivo de la información que maneja en su equipo de cómputo.

Si un equipo de cómputo requiere algún procedimiento de formateo o reinstalación de aplicaciones, por problema de infección de virus, o por algún daño sufrido, debe realizar la solicitud a través de la herramienta de soporte a usuarios, quien respaldará la información y documentos relacionados con las funciones para proceder a realizar el diagnóstico y posterior reparación.

Los colaboradores no deberán realizar alteraciones físicas o lógicas a los equipos de cómputo y dispositivos, así mismo no deberán cambiar componentes internos o externos.

El uso de dispositivos de almacenamiento externo que no sean de la Entidad es responsabilidad de los colaboradores por cuanto deberán asegurarse de que estos no contengan virus que puedan afectar a los equipos de cómputo o comprometer la infraestructura, redes, comunicaciones o servidores.

Los equipos de cómputo y dispositivos serán entregados mediante un acta de entrega donde se detallarán los componentes de software y hardware que tendrá el equipo a ser asignado. Desde este momento cada colaborador será responsable de los equipos, periféricos y accesorios asignados, su cuidado y buen uso.

En caso de que un equipo móvil (portátil, teléfono celular, periférico, accesorio) presente hurto o extravío, el colaborador deberá informar a gestión de tecnologías convergentes y la dirección jurídica y administrativa, así mismo deberá realizar la denuncia respectiva.

Cuando un colaborador finaliza su contrato con Teveandina S.A.S. – Canal Trece se deberá realiza la devolución de todos los elementos asignados, previo a esto el proceso de gestión humana deberá informar a tecnología sobre las salidas e ingresos con el fin de programar la entrega y recepción de equipos. Las devoluciones se sustentan mediante acta de entrega.

9.8 Política Sobre el uso de equipos personales (BYOD)

Las siguientes disposiciones deben ser tenidas en cuenta para el uso de los equipos personales en modalidad BYOD Bring Your Own Device), "trae tu propio dispositivo". Estas están incluidas dentro del manual de configuración equipos personales:

Serán instaladas las siguientes herramientas en los equipos de los usuarios BYOD:

- Paquete Office 365 (Word, Excel, Power Point, Teams) solo para colaboradores que cuenten con correo institucional (Hasta 5 dispositivos)
- Outlook Web
- One Drive con capacidad de almacenamiento y sincronización de 1 TB (solo para colaboradores que cuenten con correo institucional)
- Sophos Antivirus (Si cuenta con antivirus de pago se mantiene en el equipo)
- Google Chrome
- Mozilla Firefox
- Lector de pdf (Adobe, Nitro)
- 7 Zip
- VLC (Si aplica)
- Impresoras
- Carpetas de escáner
- ERP SYSMAN (en los casos que aplique)
- ORFEO (En los casos que aplique)

Los usuarios son responsables por la instalación de otro tipo de aplicaciones o uso de servicios, debido a que estos tienen control total sobre sus equipos.

El software adicional instalado en los equipos BYOD, es responsabilidad de los usuarios, antes y durante la vigencia del contrato, por cuanto se realiza la configuración de los anteriormente mencionados por el personal encargado.

El personal del proceso de tecnologías convergentes solo podrá realizar soporte sobre el funcionamiento de las herramientas instaladas, inconvenientes físicos, sistema operativo u otros programas diferentes, deben ser gestionados por los usuarios BYOD a través de servicio técnico especializado o garantías de los equipos.

La seguridad de los equipos está a cargo de cada uno de los usuarios, es importante que, si son equipos portátiles, estos estén asegurados por guayas. Al presentarse daños físicos de los equipos, cada usuario deberá hacerse cargo a través de servicio técnico particular o garantía con el proveedor.

Sobre la seguridad lógica de los equipos BYOD, es responsabilidad de los usuarios conocer y cumplir las políticas específicas en seguridad de la información y las obligaciones contractuales referidas al respecto.

En caso de que se evidencien riesgos potenciales a la seguridad de la información derivada por la propagación de virus informáticos por los equipos ingresados por los usuarios, se tomarán las medidas correspondientes de mitigación y responsabilidad que haya lugar.

Los equipos deben tener las actualizaciones y parches de seguridad sobre el sistema operativo, en caso de encontrar vulnerabilidades, los encargados del proceso de tecnologías convergentes desconectarán los equipos de la red y servicios internos.

9.9 Política de Uso del correo electrónico

Las siguientes disposiciones deben ser tenidas en cuenta para un buen uso del correo electrónico por cada uno de los colaboradores:

Las cuentas de correo no pueden ser leídas y administradas por otras personas, cuando un colaborador está ausente debe redireccionar a otra persona de su proceso, con perfiles similares, los correos electrónicos y la información gestionada.

Todos los mensajes enviados y recibidos deben contener información relacionada con las actividades de la Entidad, no pueden ser enviados correos con información que no tenga relación con el proceso a correos ajenos.

Los usuarios podrán enviar información confidencial a través de herramientas de compresión con clave (tipo ZIP), previamente controlados por los procesos de acuerdo con sus responsabilidades.

9.10 Política de Uso de Software Legal y Derechos de Autor

Todos los colaboradores solo podrán usar el software adquirido legalmente por la Entidad, en caso de presentarse algún tipo de reclamación por software ilegal, la responsabilidad será directamente del colaborador donde este instalado este software. De igual forma en presentaciones, documentos, informes y demás relacionados, los colaboradores que hagan uso de referencias deben indicar la fuente de donde se obtuvo la información.

10. ADMINISTRACIÓN DE REDES

10.1 Objetivos

Con apoyo de herramientas de administración en red, controlar las posibles interrupciones y degradación del rendimiento la red como (Malware, Gusano de Troyanos, sniffer, denegación de servicios DDos). Y Contar con una estrategia de gestión para optimizar su infraestructura existente y optimizar el rendimiento de sus aplicaciones y servicios, pronosticando crecimiento a medida que evoluciona la tecnología.

10.2 Alcance

Esta política se aplica a todas las redes, servicios de red y controles utilizados Teveandina S.A.S – Canal Trece, con el fin de proteger la información cuando esta sea utilizada para fines de transferencia vía intranet como internet

10.3 Responsabilidades

La política establece como responsable el encargado del área, como eje central, de las configuraciones y disposiciones del software necesario, equipos de comunicación, mantenimiento de los comunicados los equipos de cómputo. Y su vez el encargado de investigar y proponer soluciones de redes y comunicación. Bajo parámetros de seguridad establecerá apoyo con el oficial de seguridad.

10.4 Generalidades

Para garantizar la integridad y seguridad en los datos, se hace necesario implementar controles para el acceso a la red de la Entidad, así pueden ser utilizados de forma correcta todos los recursos de red previniendo fugas, intrusiones y riesgos sobre los activos de información.

Es responsabilidad del personal encargado configurar y controlar los accesos para los usuarios debidamente identificados y registrados. Para este fin deben diseñados los procedimientos adecuados para el acceso a la red alámbrica e inalámbrica.

10.5 Política de Utilización de los servicios de red

Serán controlados los servicios de red internos y externos, a partir de solicitudes formales hechas por los líderes de proceso, con el fin de llevar control sobre los ingresos. Es responsabilidad del proceso de tecnologías convergentes otorgar los accesos a servicios y recursos de red para los usuarios autorizados a través de una solicitud hecha por la herramienta de soporte a usuarios.

10.6 Política de Conexiones de red

Las conexiones de red serán administradas a través de herramientas informáticas para establecer mecanismos de autenticación seguros, perfilar y controlar la red de datos interna. Así mismo, debe contar con un esquema de segmentación para controlar el acceso y garantizar la confidencialidad, integridad y disponibilidad de la información. Deben ser separadas las redes inalámbricas de las redes con conexión alámbrica.

10.7 Política de Autenticación para conexiones externas

El proceso de tecnologías convergentes tendrá la responsabilidad de asignar según corresponda, conexiones y medios de autenticación a terceros según las necesidades de los demás procesos, para ello cada líder de proceso deberá realizar la solicitud vía la herramienta de soporte a usuarios, con el fin de evaluar su viabilidad para autorización de instalación y configuración de aplicativos.

10.8 Política de Acceso a Internet

El acceso a Internet debe ser usado para propósitos autorizados, el proceso de tecnologías convergentes determinará a través de perfiles, el acceso apropiado a sitios web, servicios en la nube, herramientas y demás que hagan uso de Internet.

Es responsabilidad de los usuarios hacer un buen uso de este servicio y evitar prácticas que puedan comprometer los servicios tecnológicos, sistemas de información e infraestructura de la Entidad. Así mismo, deberán informar el acceso a contenidos y servicios no autorizados los cuales no correspondan a sus funciones.

Son usos no aceptables del servicio, entre otros: enviar o descargar información de gran tamaño que no corresponda a sus funciones ya que esto puede congestionar la red. Así

mismo no es permitido la descarga, envío y visualización de contenidos que atenten contra la integridad de personas, la Entidad u otras instituciones.

No se permite acceso a páginas con contenido para adultos, pornografía, hackers, suplantaciones, juegos, conexiones peer to peer redes sociales (Facebook, Instagram, Snapchat, YouTube), siempre y cuando sean necesarias para el desarrollo de sus funciones. Para ello deben ser solicitadas por el líder de proceso y autorizadas por el ESI.

Todos los invitados que requieran conexión a Internet dentro de la Entidad deben realizarlo a través de la red inalámbrica de invitados y cumplir con las políticas de seguridad de la información establecidas, asumiendo responsabilidad ante su incumplimiento y acciones correspondientes.

10.9 Política de Redes Sociales y Mensajería Instantánea

la presente política entrega los lineamientos generales para proteger adecuadamente la información, al utilizar nuestros servicios de mensajería Instantáneas y redes sociales por usuarios autorizados.

La Información publicada o divulgada en Internet de cualquier manera por los funcionarios de Teveandina Canal Trece o contratistas, creado bajo nombres propios en redes sociales como: twitter, Facebook, youtube, likelink, blogs, Instagram, etc. Se discurre como fuera de alcance por las políticas establecidas del CID (confiabilidad, integridad, disponibilidad), y los perjuicios y daños puedan causar serán de completa responsabilidad de la persona que la haya creado.

Todo contenido e información distribuida en cualquier plataforma como redes sociales, de contenido institucional deber ser previamente autorizado por los diferentes jefes y áreas administrativas para ser socializada con los estándares instruccionales

10.1 Política de Conexión Red Privada Virtual (VPN)

- El acceso al correo electrónico y los aplicativos Web institucionales se hará normalmente a través de los Navegadores.
- Las conexiones remotas a los recursos informáticos deberán hacerse a través de VPN, las cuales deben ser configuradas por la oficina de tecnologías de la información y las comunicaciones.
- Los equipos de cómputo y su conexión a la VPN deben ser asignados por la Corporación y deben cumplir con una línea base definida en cuanto a configuración, controles y software instalado.
- Para el trabajo en casa se permitirá el uso de equipos personales BYOD, bajo el compromiso de uso de software legal y antivirus actualizado y de requerirse se creará conexión VPN para acceso a los recursos autorizados.
- En los equipos de cómputo de funcionarios y BYOD, no se deberá almacenar información corporativa. Esta información deberá quedar en un repositorio en un servidor de archivos definido para tal fin, en donde se controle el acceso. Para este caso la Corporación tiene disponible la intranet, el One Drive, SharePoint (nube privada Corporación) y/o servidores
- Si la clasificación de la información que produzca procese o transfiera el usuario a través de a la VPN, se deben celebrar acuerdos de confidencialidad o de no divulgación.

- La contraseña de inicio de sesión en el equipo de cómputo de los funcionarios y BYOD debe tener una vigencia definida de acuerdo con las políticas de seguridad de la información.
- La base de firmas y definiciones del producto de protección antivirus debe actualizarse cuando el equipo de cómputo de funcionario y BYOD se conecta desde el sitio remoto.
- El equipo de cómputo del funcionario y BYOD debe descargar y aplicar las actualizaciones de seguridad del sistema Operativo y otras actualizaciones de software que requiera para sus funciones.
- Los funcionarios y BYOD deben aceptar la política de uso y restricción de software. Esta señala que no pueden instalar ningún software en el equipo o usar alguno que se encuentra por fuera de la línea base definida por la Oficina de las Tecnologías de la Información y las Comunicaciones.
- El usuario de teletrabajo debe conocer y cumplir las políticas de seguridad de la información y de protección de datos personales establecidas por Teveandina Canal Trece.

11. ADMINISTRACIÓN DE PERFILES Y CONTROL DE ACCESO

11.1 Objetivos

La política contempla la prevención del acceso no autorizado a los sistemas de información físicos y lógicos. Implementando seguridad de acceso a usuarios con tecnologías de autenticación. Creando así cultura organizacional, en la que los usuarios sean responsables de su propio uso de registros y contraseñas.

11.2 Alcance

Las pautas y estándares definidas en esta política se aplican a todos los empleados. Contratistas y Terceros con Acceso a los Sistemas de Información Teveandina S.A.S – Canal Trece, Se mantendrá el seguimiento para mitigar o evitar fugas de información a procesos no controlados.

11.3 Responsabilidades

Servicios de información multiusuario con procedimientos para la asignación de permisos de acceso a sistemas, como bases de datos y Internet o redes externas. Uso de computación móvil, trabajo remoto. Análisis y propuesta de medidas para un control de acceso efectivo. Corroborando y contrastando con el cumplimiento de las políticas establecidas y relacionadas con el control de acceso. creación de usuarios, gestión de derechos, gestión de contraseñas, Uso de servicios de red, uso controlado de software del sistema y correo electrónico Herramientas institucionales y/o colaborativas.

11.4 Generalidades

Esta política establece aspectos sobre los protocolos para controlar el ingreso a los sistemas de información, bases de datos y otros servicios a partir de perfiles.

Todos los colaboradores deben tener conciencia sobre el uso de los perfiles y accesos a servicios tecnológicos y sistemas de información para prevenir alteraciones sobre estos.

Esta política a su vez está dirigida al personal de tecnologías convergentes que gestiona los servicios tecnológicos y sistemas de información, con el fin de crear cuentas de usuario y accesos de acuerdo con los perfiles adecuados.

11.5 Política Registro de Usuarios

El personal encargado del proceso de tecnologías convergentes debe especificar el registro de usuarios a través de las siguientes condiciones:

- Nombre que identifica al usuario del sistema
- Establecer una contraseña con longitud de 6 o más caracteres alfanuméricos.
- Permitir la vigencia para las contraseñas en un tiempo máximo de 30 días.

El registro de los usuarios debe ser solicitado por los supervisores de proceso a través de la herramienta de soporte a usuarios, especificando los datos de la persona a registrar dentro del sistema de información o servicio tecnológico.

11.6 Política de Privilegios de Usuario

Deben ser limitados y controlados los perfiles de usuario de los colaboradores ya que el uso indebido de los mismos permite que existan fallos en los sistemas de información y servicios tecnológicos por accesos inadecuados. En todos los sistemas y servicios multiusuario que requieran protección contra accesos no permitidos, los líderes de proceso deben especificar la asignación de privilegios según corresponda.

11.7 Política de Contraseñas de Usuario

Deben ser establecidas contraseñas individuales a cada usuario, sobre estas el equipo del proceso de tecnologías convergentes debe garantizar su protección mediante métodos de cifrado.

Las contraseñas deben contener como mínimo una longitud de 6 caracteres, incluyendo mayúsculas, minúsculas, números, caracteres especiales, así mismo los sistemas y servicios deben permitir cambio 1 vez cada 30 días.

Es deber de todos los colaboradores dar un buen uso a las contraseñas entregadas, por tanto, estas no pueden ser compartidas ni reveladas por correo electrónico, telefónicamente o ser expuestas en algún medio físico dejándolas a la vista.

Los colaboradores deben reportar al proceso de tecnologías convergentes cualquier incidente presentado con el uso indebido de las contraseñas.

Las contraseñas de servicios, sistemas e infraestructura tecnológica que vienen con contraseñas por defecto deben ser cambiadas por los encargados de su administración y operación, dejando registro en la base de datos de uso exclusivo del proceso de tecnologías convergentes.

Las contraseñas de administración de los servicios tecnológicos y sistemas de información en operación deben ser cambiadas trimestralmente, así mismo el acceso a estos debe ser autorizado por el proceso de tecnologías convergentes.

Las contraseñas de las cuentas de servicios brindados por terceros (redes sociales, servicios y herramientas en línea) deben ser gestionados por los encargados de su administración y

uso. De tal forma que se debe garantizar cambios periódicos en las contraseñas de forma semanal o diaria dependiendo el caso.

11.8 Política de Derechos de acceso a los Usuarios

El área encargada junto al ESI (Equipo de Seguridad de la Información) tienen como obligación garantizar una revisión periódica de los privilegios de acceso en todos los usuarios de servicios tecnológicos y sistema de información, con el fin de actualizar accesos y perfiles sobre estos.

12. USABILIDAD DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

12.1 Objetivo

El propósito de esta política es aclarar las responsabilidades y los controles organizacionales relacionados con el uso de medios extraíbles. Incluye unidades flash USB, discos duros externos, dispositivos móviles utilizados como almacenamiento externo y medios ópticos (CD, DVD, etc.) y otros dispositivos informáticos que no están físicamente conectados a las unidades de procesamiento. El objetivo es miniar el riesgo de pérdida o divulgación de información confidencial y reduzca el riesgo de infección o destrucción de data.

12.2 Alcance

La política busca la interacción de todos los activos y recursos, tanto para Tecnología de la Información como para tecnología de Operaciones, sistemas operativos, software de aplicaciones, hardware de cómputo, redes y servicios en nube, y/o todo equipo manejado por Teveandina S.A.S. – Canal Trece (de propiedad, bajo arrendamiento o personal) o donde residan información de la entidad.

12.3 Responsabilidades

Asegurar la política vigente con sus respectivas actualizaciones, ajustes, comentarios y reclamaciones. proporcionadas en los servicios tecnológicos y lineamientos establecidos en la presente política. Se detalla que cada usuario es el responsable de cumplir con esta política, y Teveandina S.A.S. – Canal Trece de controlar su cumplimiento.

12.4 Generalidades

Para Teveandina S.A.S. – Canal Trece es importantes garantizar la protección de los activos de información gestionados a través de unidades de almacenamiento externo. Esta política está dirigida a todos los colaboradores que hacen uso de unidades de almacenamiento removibles como CD´s, DVD´s, tarjetas de memoria, unidades personales de almacenamiento, cámaras para la captura fotográfica y de video, entre otros.

12.5 Política de Gestión y disposición

Todos los dispositivos y unidades de almacenamiento externos (CD´s, DVD´s, tarjetas de memoria, unidades personales de almacenamiento, cámaras para la captura fotográfica y de video, entre otros), los cuales sean usados por los colaboradores en virtud de sus funciones, deberán ser controlados por el proceso de tecnologías convergentes desde su acceso, uso y devolución.

Los dispositivos y unidades de almacenamiento externo deben tener un registro controlado y actualizado por los procesos encargados.

El equipo de tecnologías convergentes podrá restringir los dispositivos y unidades de almacenamiento externos propiedad de la Entidad que incurra en riesgos a la infraestructura, servicios y sistemas de información, debido a la presencia de virus informáticos o problemas en su funcionamiento. Es importante realizar seguimiento a todos los dispositivos removibles con el fin de garantizar la transferencia de la información sobre aquellos que estén próximos a cumplir con su vida útil.

Los retiros de dispositivos y unidades de almacenamiento externos (CD´s, DVD´s, tarjetas de memoria, unidades personales de almacenamiento, cámaras para la captura fotográfica y de video, entre otros) deben ser reportados y controlados por los procesos que hacen uso de estos, con el fin de llevar trazabilidad en caso de perdidas o daños que comprometan la información allí almacenada.

Se deben establecer controles como registro en bitácora y revisión por herramienta de antivirus de los discos externos proporcionados por terceros, con el fin de prevenir posibles intrusiones por virus informáticos presentes en estos dispositivos.

12.6 Política de Proceso de borrado seguro

Los dispositivos y unidades de almacenamiento externos (CD, DVD´s, tarjetas de memoria, unidades personales de almacenamiento, computadoras, cámaras para la captura fotográfica y de video, entre otros) propiedad de la Entidad o de terceros autorizados, deberán estar sujetos a los procedimientos de soporte.

El proceso de tecnologías convergentes deberá establecer un proceso de borrado seguro a través de herramientas para tal fin, y así garantizar que la información almacenada no pueda recuperarse, así mismo los dispositivos que vayan a ser reutilizados deben seguir el procedimiento de borrado seguro (aplica para equipos propios y alquilados).

12.7 Política de Transporte y transferencia

Los dispositivos y unidades de almacenamiento externos (CD´s, DVD´s, tarjetas de memoria, unidades personales de almacenamiento, computadores, cámaras para la captura fotográfica y de video, entre otros) que sean transportados fuera de la Entidad, deberán cumplir con los protocolos señalados por el proceso de tecnologías convergentes, indicando si deben ejecutarse técnicas de cifrado.

El transporte debe realizarse a través de medios seguros de acuerdo con las condiciones y medidas necesarias para garantizar que los dispositivos y unidades de almacenamiento sean transportados de forma adecuada.

13. ADMINISTRACIÓN DE BACKUP

13.1 Objetivos

Definir lineamientos y controles generales para los sistemas de información, Infraestructura TI y componentes de seguridad. Dando como objetivo los Backup, almacenamiento (Fuera de Sitio y Local) y restauración de la información en caso de desastre natural o ataque cibernético.

13.2 Alcance

El alcance de esta política comienza con la identificación de copias de seguridad tales como, carpetas, archivos, imágenes, audios, herramientas de apoyo, dispositivos o unidades de tecnología, y, por último, pero no menos importante el monitoreo de estos. Con previamente designación de controles y actividades que se deben preparar, al momento de la extracción.

13.3 Responsabilidades

Define en primera instancia que cada usuario es el primer encargado de vigilar y proteger la información que reposa en sus equipos electrónicos, Teveandina S.A.S. – Canal Trece, ofenderá repositorios (sharepoint) como mecanismo de apoyo, para salvaguardar esta información bajo los pilares de CID

13.4 Generalidades

El proceso de copias de seguridad garantiza mantener la información segura ante riesgos internos y externos.

El proceso de gestión de tecnologías convergentes tiene debe implementar la generación periódica de backups bajo los estándares necesarios y garantizar una adecuada custodia de estos.

13.5 Política Generación de backups

Con el fin de proteger la información sobre todos los procesos de la entidad deben ser tenidos en cuenta los siguientes aspectos:

Establecer como medida de seguridad la sincronización de los archivos de gestión a través del servicio de almacenamiento en la nube incluido en las cuentas de correo electrónico (One Drive), con el fin de mantener una copia de respaldo ante posibles pérdidas de información por fallas en los equipos de cómputo.

Es deber de cada colaborador mantener los archivos almacenados en One Drive o en la carpeta "documentos" del sistema operativo (en caso de no tener cuenta de Office 365), así como solicitar asistencia para su realización.

El proceso de tecnologías convergentes debe revisar trimestralmente la sincronización de los documentos en los servicios en la nube y de forma local en los equipos de cómputo, así mismo los colaboradores deberán entregar al finalizar el contrato una copia de los archivos al supervisor para garantizar continuidad en la información de gestión de los procesos.

Se deben disponer de ambientes de pruebas necesarios para realizar restauraciones periódicas de las copias de seguridad, con el fin de garantizar la disponibilidad de la información crítica.

Definir dentro del procedimiento de copias de seguridad las condiciones de rotulado, medios de almacenamiento, tiempos de retención, reutilización de los medios de almacenamiento y destrucción.

Se deben realizar copias de la información de los servidores, bases de datos, servidores web, sistemas de información, configuraciones básicas, aplicaciones, ambientes de desarrollo, dispositivos de red y comunicaciones.

Realizar una copia de seguridad completa anual de los servidores, bases de datos, servidores web, sistemas de información, configuraciones básicas, aplicaciones, ambientes de desarrollo, dispositivos de red y comunicaciones.

Las copias de seguridad deben realizarse en horario laboral no hábil a través de procesos automáticos.

Se deben conservar los medios de almacenamiento bajo las condiciones ambientales necesarias.

El personal encargado debe conocer y utilizar adecuadamente software para la generación de copias de respaldo, así como generar rótulos para almacenamiento físico y lugares de custodia.

13.6 Política Registro de backups

El proceso de gestión de tecnologías convergentes deberá controlar las copias de seguridad de los sistemas de información, servicios tecnológicos e infraestructura con el fin de conocer cuáles de los activos de información están siendo respaldados y su lugar de almacenamiento.

Las copias de seguridad deben ser probadas por lo menos dos veces al año con el fin de verificar su integridad y efectividad.

Se deben configurar las herramientas para la realización de las copias de seguridad para que esta genere eventos completados y fallidos sobre estas.

Mantener una copia de seguridad de los servidores con una periodicidad de mínimo 24 horas.

Monitorear rendimiento y alcance de las bases de datos con el fin de garantizar la información respaldada.

14. SEGURIDAD FÍSICA Y AMBIENTAL

14.1 Objetivo

Contar los recursos humanos necesarios y ubicaciones disponibles para efectuar las actividades de la presente política, lo cual el personal debe estar dotado con las herramientas o elementos necesarios para la ejecución de las actividades dentro de este, Adicionalmente el servicio de soporte técnico permanente para los sistemas involucrados en este procedimiento, sin excepción y con previa vigilancia del encargado de área.

14.2 Alcance

Este procedimiento está destinado específicamente a los funcionarios que están comprometidos con Teveandina S.A.S. – Canal Trece. El propósito de la política es asegurar el correcto funcionamiento del mantenimiento. información de la empresa y Disponibilidad de la información en sí.

14.3 Responsabilidades

La política refiere únicamente al personal autorizado o con previa supervisión del área encargada, programadores, personal de infraestructura y demás personal que está en

contacto directo. Los visitantes que ingresen serán de previa autorización del jefe del área de Informática o del responsable encargado de realizar alguna actividad.

14.4 Generalidades

La seguridad física y ambiental minimiza los riesgos presentados debido a interferencias sobre información y los procesos de la Entidad. Dentro del centro de cómputo se resguarda la información derivada de transacciones, configuraciones de servicios y comunicaciones, así pues, se debe garantizar un correcto uso y funcionamiento evitando suspensiones en el servicio.

14.1 Política Seguridad Centro de Datos y Centro de Cableado

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas por Teveandina Canal Trece

14.2 Política Normas de uso para el Centro de Cómputo

Las siguientes normas describen los procedimientos que deben ser tenidos en cuenta para un correcto uso del Centro de Cómputo:

El centro de cómputo y el Datacenter no deben estar ubicados en un lugar con alto tráfico de personas bajo condiciones básicas para su uso (piso, techo, puertas, cableado).

El personal encargado debe establecer a través de una planilla de registro, el acceso a colaboradores no autorizados a las instalaciones del Centro de Computo.

Cuando un colaborador no autorizado requiera ingresar al Centro de Computo debe solicitar autorización al proceso de tecnologías convergentes donde sea especificada la actividad a realizar con presencia del personal encargado.

El personal encargado debe llevar el registro de todos los ingresos autorizados al Centro de Cómputo.

Los equipos informáticos ajenos ingresados al Centro de Cómputo restringidos deberán ser registrados.

Al realizar mantenimientos en los equipos del Centro de Cómputo se debe avisar anticipadamente a todos los colaboradores para proteger la continuidad del negocio.

14.3 Política De Escritorios Y Pantallas Limpias

Los siguientes aspectos deben ser tenidos en cuenta para la protección de la información ubicada en escritorios, puestos de trabajo, documentos físicos, medios magnéticos, usados por los colaboradores de la Entidad.

Los puestos de trabajo deben estar ubicados de tal forma que no queden expuestos al acceso de personas externas, con el fin de proteger los equipos informáticos y los documentos usados a diario.

Siempre que colaborador se ausente de su puesto de trabajo debe bloquear de forma segura el equipo de cómputo y guardar en los cajones bajo llave, documentos, medios magnéticos u ópticos que tengan información sensible.

Al finalizar la jornada laboral, los colaboradores deben guardar en un lugar seguro documentos y medios que contengan información de uso interno de la Entidad.

Las pantallas de autenticación a la red interna únicamente deben solicitar nombre de usuario y contraseña sin mostrar otro tipo de información.

15. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

15.1 Objetivo

Las políticas establecen los controles de seguridad de la información necesarios dentro del proceso. continuidad del negocio o recuperación ante desastres y sistemas y cambios en herramientas y procesos de soporte, procedimientos e implementaciones manteniendo controles de seguridad de la información existentes en circunstancias adversas. finalmente, alinear los dominios para controles de seguridad en información que no se puede almacenar en circunstancias adversas.

15.2 Alcance

Desarrollar y aprobar un plan, una respuesta y una recuperación documentados que detallen cómo Teveandina S.A.S.– Canal Trece. gestiona los eventos disruptivos y mantiene la seguridad de la información dentro de los límites prescritos en base a los Objetivos de Continuidad de la Seguridad y la información definida en esta política.

15.3 Responsabilidades

Esta política comprende la previa responsabilidad de Teveandina S.A.S.– Canal Trece. Y sus colabores, debido a las posibles consecuencias para asegurar la cadena de valor de la entidad. Esta continuidad de negocio es proyectada en caso de un evento que afecte el funcionamiento normal del negocio o proceso importantes.

15.4 Generalidades

Teveandina S.A.S. Canal Trece debe garantizar las necesidades básicas para la continuidad de la operación ante situaciones tales como desastres naturales y eventos adversos.

Para ello, se debe disponer de un sitio alterno que permita operar los servicios tecnológicos, herramientas y sistemas de información críticos, a través de los lineamientos establecidos por las políticas de seguridad de la información descritas.

Los aspectos relacionados con la recuperación ante situaciones adversas deberán estar relacionadas en los planes de contingencias, incluyendo aspectos referidos a la protección de los activos de información y su recuperación para dar continuidad a la operación. Adicional se debe crear un plan de contingencia para los servicios tecnológicos, herramientas y sistemas de información vigentes.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 Objetivo

Gestionar todos los incidentes de seguridad de la información apropiadamente, reportados por el personal de Teveandina – Canal Trece, con el fin de dar cumplimiento a los instructivos establecidos.

16.2 Alcance

La presente política aplica para todo el personal de planta, contratistas y terceros de Teveandina – Canal Trece que detecten un evento o incidente de seguridad de la información el cual puedan reportar, adecuadamente, de acuerdo con los procedimientos establecidos por el área de seguridad.

16.3 Responsabilidades

El Directorio de la empresa es responsable por difundir la presente política a todo el personal, independiente del cargo que desempeñe.

El personal de la empresa es responsable por dar cumplimiento a la presente política y reportar los eventos de seguridad que detecte al responsable de seguridad de la información, siguiendo los procedimientos operativos establecidos para tal fin.

El responsable de seguridad de la información debe velar por el cumplimiento de esta política.

16.4 Generalidades

Los incidentes de seguridad de la información se definen como el acceso no autorizado, intento de acceso, uso, divulgación, modificación o destrucción de la información; interrupción del funcionamiento normal de redes, sistemas o recursos informáticos; o violaciones a las políticas de seguridad de la información de las entidades administrativas relacionadas con el mejoramiento y mantenimiento al SGSI. El informe de incidentes permite una respuesta sistemática a los incidentes, la reducción de incidentes, la recuperación rápida y eficiente de las operaciones, la reducción de la pérdida de información, las interrupciones del servicio y el manejo y la gestión adecuados de los incidentes. Cuestiones disciplinarias y legales que puedan surgir en el proceso.

16.5 Política Lineamientos Y Elaboración Para El Tratamiento Del Incidente

• ***Gestión de seguridad***: Planificar la gestión de las debilidades. El plan para sistemas operativos, bases de datos y aplicaciones ayudará a las autoridades a determinar, verificar y crear seguridad de la

• ***Ciberseguridad***: Proteger los equipos y administrando proactivamente todos los componentes de seguridad. Revisar las reglas configuradas en el firewall una vez por semana con apoyo del ingeniero de TI. El hardware FW y el software antivirus deben actualizarse con actualizaciones de firmas. Todos los proyectos de seguridad y red deben sincronizarse y enviar sus registros a un equipo central de recopilación de registros para cada análisis.

• ***Código antimalware***: Los dispositivos sin excepción de infraestructura (servidores y equipos de usuario) deben estar habilitados con software antivirus y antimalware con firmas actualizadas.

• ***Concientización y capacitación de usuarios***: Capacitación y sensibilización a todo el personal del canal, incluidos los lideres y gerente de Teveandina – Canal Trece, publicar la política de seguridad actual y llevar a cabo estas actividades de concientización por parte de expertos o entidades educativas en seguridad de la información.

17. CRIPTOGRAFÍA

17.1 Objetivo

Salvaguardar la confidencialidad, integridad, autenticidad y no repudio de la información, mediante implementación de técnicas y sistemas en análisis de riesgos. Garantizando que solo las partes autorizadas puedan acceder y utilizar la información, previniendo el acceso no autorizado y la manipulación de los datos durante su almacenamiento, transmisión y procesamiento.

17.2 Alcance

Abarcar múltiples aspectos de la seguridad de la información y las comunicaciones digitales. En esencia, para proteger la confidencialidad, integridad, autenticidad y no repudio de los datos en diversas aplicaciones. Esto incluye la protección de información sensible mediante la aplicación de algoritmos para cifrar y descifrar datos, así como la gestión segura de claves. Además, para garantizar la seguridad de las comunicaciones, tanto en redes públicas como privadas, mediante la autenticación de usuarios y dispositivos, y la protección contra el acceso no autorizado y la manipulación de datos. Se extiende todas las medidas y técnicas utilizadas a Teveandina – Canal Trece, para asegurar la seguridad de la información y las comunicaciones en entornos digitales.

17.3 Responsabilidades

Las responsabilidades de la criptografía implican la aplicación de técnicas y protocolos para asegurar la confidencialidad, integridad, autenticidad y no repudio de la información en entornos digitales. Esto incluye la selección y configuración adecuada de algoritmos criptográficos, la gestión segura de claves, la implementación de medidas de seguridad criptográfica en sistemas y comunicaciones, así como la detección y mitigación de posibles vulnerabilidades en los sistemas criptográficos. Además, el responsable de la criptografía debe garantizar el cumplimiento normativo y la concienciación sobre la importancia de la seguridad criptográfica dentro de la organización. En resumen, las responsabilidades de la criptografía comprenden todas las acciones necesarias para proteger la información sensible y garantizar la seguridad de los sistemas y comunicaciones digitales.

17.4 Generalidades

Conceptos fundamentales y principios básicos que conforma la seguridad informática. Esto incluye aspectos como los objetivos (confidencialidad, integridad, autenticidad, no repudio, firmas digitales), los tipos de técnicas (cifrado simétrico, cifrado asimétrico, funciones de resumen, firmas digitales), la gestión de claves, algoritmos y su aplicación en la protección de la información y las comunicaciones digitales. En resumen, son conceptos básicos y fundamentales que constituyen su campo de estudio y aplicación en la seguridad de la información.

17.5 Política sobre el uso de controles criptográficos para la protección de la información.

- ***Utilización de Controles Criptográficos:***

a) Protección de acceso a sistemas, datos y servicios.
b) Transmisión de información clasificada fuera del ámbito de la Teveandina S.A.S. Canal Trece.
c) Salvaguardar información basándose en evaluaciones de riesgos realizadas por el Propietario de la Información y el responsable de Seguridad Informática.
d) Procedimientos para la gestión de claves, la recuperación de información cifrada en caso de pérdida o compromiso de claves, así como para el reemplazo de estas.
e) El responsable del SGSI propondrá la asignación de credenciales y el tiempo de actualización de estas
f) Se utilizarán los algoritmos de cifrado y tamaños de clave especificados por el responsable del SGSI.

- ***Cifrado***: El nivel de protección necesario se determinará mediante una evaluación de riesgos, considerando el tipo y calidad del algoritmo de cifrado y la longitud de las claves. Se aplicarán controles criptográficos teniendo en cuenta regulaciones para la exportación e importación de tecnología criptográfica.

- ***Firma Digital:*** Las firmas digitales garantizan la autenticidad e integridad de documentos electrónicos. Se protegerán las claves privadas y se recomendará no utilizar las claves para firmar digitalmente en procesos de cifrado. Se considerará la legislación vigente para la validez legal de las firmas digitales.

- ***Servicios de No Repudio:*** Se utilizarán para resolver disputas sobre transacciones electrónicas, evitando la negación de estas.

- ***Administración de Claves:*** Se implementará un sistema de gestión de claves para ambos tipos de técnicas criptográficas: clave secreta y clave pública. Se establecerán normas, procedimientos y métodos para generar, distribuir, almacenar, cambiar, revocar, recuperar, archivar y destruir claves. Se aplicarán fechas de inicio y caducidad para reducir el riesgo de compromiso. La administración de certificados de clave pública será llevada a cabo por una Autoridad de Certificación o Certificador.