Políticas de Seguridad de la Información

Teveandina Ltda. – Canal Trece

Revisiones y control de cambios

Titulo	**Políticas de Seguridad de la Información, TEVEANDINA LTDA. – CANAL TRECE**
Autores	Gonzalo Joya Santana, Miller Dorado, Cristian Ostos
Tema	Políticas de Seguridad de la Información
Fecha de Elaboración	Noviembre 2019
Formato	PDF
Versión	1.0
Palabras Relacionadas	MSPI, gestión de riesgos, políticas de seguridad de la información

Control de Cambios			
Fecha	**Autores**	**Versión**	**Cambio**
Noviembre 2019	Gonzalo Joya Miller Dorado Cristian Ostos	1.0	Versión Inicial
Abril 2020	Gonzalo Joya Miller Dorado Cristian Ostos	1.0	Versión con observaciones lideres de proceso

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.

- Riesgo. Es la probabilidad de ocurrencia sobre un evento en el sistema de información con consecuencias negativas.

- 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.

3. Alcance

La política aplica para todos los colaboradores de Teveandina Ltda – Canal Trece y demás que desempeñen funciones con la Entidad.

4. Marco regulatorio y normativo

Teveandina Ltda – 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- 27002:2013

5. Equipo en Seguridad de la Información (ESI)

Se creará el equipo de Seguridad de la Información (ESI) para la administración, gestión y divulgación de esta política de seguridad y los sistemas que la soportan.

El comité estará integrado por los siguientes miembros:

- Gerente
- CIO TI
- Director jurídico y administrativo
- Líder de planeación
- Personal encargado seguridad de la información
- Personal encargado de la infraestructura y las comunicaciones
- Equipo de Arquitectura y Gobierno Digital

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.

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).

7. Política de uso y clasificación de los activos de información

7.1 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

7.2 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.

7.3 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.

8. Política para gestión de Sistemas de Información y Servicios Tecnológicos

8.1 Generalidades

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

8.2 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 a 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

Ltda – 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 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 Ltda. – 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.

8.3 Sobre el uso de equipos personales

Las siguientes disposiciones deben ser tendidas 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 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.

8.4 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 a sus responsabilidades.

8.5 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.

9. Política de Administración de Redes

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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. Política de Administración de Perfiles y Control de Acceso

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

11. Política sobre el uso de dispositivos de almacenamiento externo

11.1 Generalidades

Para Teveandina Ltda. – Canal Trece es importante 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.

11.2 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.

11. 3 Proceso de borrado seguro

Los dispositivos y unidades de almacenamiento externos (CD, DVD´s, tarjetas de memoria, unidades personales de almacenamiento, 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).

11.4 Transporte y transferencia

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) 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.

12. Política para Administración de Backup

12.1 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.

12.2 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.

12.3 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.

13. Política de acceso al Centro de Cómputo

13.1 Generalidades

La seguridad física 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.

13.2 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. 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. Política de continuidad del negocio

Teveandina Ltda. 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.


Tr-ce