DUEÑO DE PROCESO: Director de Sistemas

Elaborado por:	**Revisado por:**	**Aprobado por:**
Fredy E. Castillo H.	Andrés Vega Alvarado	Mauricio Ruiz
Cargo:	**Cargo:**	**Cargo:**
Director de Sistemas	Director de Procesos	Gerente General
Fecha:	**Fecha:**	**Fecha:**
AAAA-MM-DD	AAAA-MM-DD	AAAA-MM-DD

VIGENCIA	CONTROL DE CAMBIOS
OCT 14	Elaboración del documento. Este documento elimina la política de actuación #9 del Manual de Calidad, ya que en el capítulo 7 involucra todas sus políticas.
NOV 18	**Revisión y actualización del documento y sus directrices.**

1. INTRODUCCIÓN

La Dirección de Sistemas Cesvi Colombia S.A. determina la información como un activo de alta importancia para la entidad; esta permite el desarrollo continuo de la Misión y el cumplimiento de la misma; a partir de esta necesidad se requieren implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

El presente manual establece las políticas que deben ser adoptadas por los trabajadores y terceros que presten sus servicios o tengan relación con Cesvi Colombia.

La seguridad de la información es para Cesvi Colombia, una labor prioritaria que exhorta a todos a velar por el cumplimiento de las políticas establecidas en el presente manual.

2. OBJETIVO

Establecer el marco y ser el modelo para la realización de las diferentes actuaciones en materia de seguridad de la información, así como también presentar en forma clara y coherente los elementos que conforman la política de seguridad la cual deben conocer, acatar y cumplir todos los trabajador y terceros que presten sus servicios o tengan relación con la empresa.

Establecer las acciones necesarias para que los activos informáticos de Cesvi Colombia S.A. dispongan de un nivel de protección eficaz, proporcional, coherente y adecuado a la dimensión y a los intereses de la Compañía, permitiendo alcanzar y mantener niveles de riesgo aceptables.

Se procurará la optimización y racionalización de los recursos informáticos de tal manera que se alcance el nivel adecuado y necesario de protección para la información y activos informáticos de Cesvi Colombia S.A.

3. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, trabajadores y terceros que presten sus servicios o tengan relación con Cesvi Colombia, para el adecuado cumplimiento de sus funciones y para conseguir un nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas por la Dirección de Sistemas y aprobadas por la Gerencia General.

Esta política tiene alcance en todos los procesos de Cesvi Colombia S.A. en la medida que el ambiente de TI se vea involucrado.

4. APLICABILIDAD DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información de Cesvi Colombia S.A. aplica y es de obligatorio cumplimiento para la Gerencia, Directores, trabajadores y en general a todos los usuarios de la información que permitan el cumplimiento de la Misión de Cesvi Colombia.

5. DEFINICIONES Y ABREVIATURAS

Activo: Cualquier cosa que tiene valor para la organización, también se entiendo por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Se pueden clasificar de la siguiente manera:

- **Datos:** son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en Cesvi Colombia
- **Aplicaciones:** es todo el software que se utiliza para la gestión de la información
- **Personal:** son todos los empleados, personal contratado, los clientes, usuarios y en general todos aquellos que tengan acceso de cualquier manera a los activos
- **Servicios:** son el conjunto de actividades que buscan satisfacer una necesidad tanto a clientes internos como externos.
- **Tecnología:** son todos los equipos utilizados para gestionar la información y las comunicaciones
- **Instalaciones:** son todos los lugares en los que se alojan los sistemas de información
- **Equipamiento auxiliar:** son todos aquellos activos que dan soporte a los sistemas de información y que no se incluyen en los tipos definidos anteriormente

Almacenamiento en la Nube: Es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet pueden ser aplicaciones o servicios.

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

Amenaza: Causa o fuente potencial de daño a los activos informáticos.

Daño: Perdida material y/o intangible producida como consecuencia directa o indirecta de la materialización de una amenaza.

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

Disponibilidad: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad o persona.

Evento: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas.

Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo. La gestión de los riesgos incluye, por norma general, la valoración del riesgo, tratamiento del riesgo, aceptación de riesgos y comunicación de los mismos.

Incidente de Seguridad: Cualquier hecho o situación que produce un daño o menoscabo de los activos informáticos de Cesvi Colombia S.A o que supone una violación de la política de seguridad de la información.

Información: Activo esencial para las actividades de la organización y en consecuencia debe ser objeto de una protección adecuada. Esta puede existir de varias maneras; puede ser impresa, almacenada electrónicamente, transmitida por correo o medios electrónicos, expuesta en multimedia, etc.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso, también puede ser interpretada como la propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Peligro: Hecho o fenómeno que puede ser causante de daños. Origen de un potencial riesgo. Sinónimo de riesgo próximo o inminente.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Riesgo: Combinación de la probabilidad de un suceso y su ocurrencia. Término que suele utilizarse solo en caso de que exista, al menos, una posibilidad de consecuencia negativa.

Seguridad: Condición conseguida cuando los activos informáticos están protegidos contra los riesgos.

Sistema SAP BUSINESS ONE (S.B.O): Sistema implementado por Cesvi Colombia para mejorar los procesos administrativos, financieros, comerciales y de servicios.

Usuario: Se refiere a todos los trabajadores permanentes o temporales y cualquier otra persona o entidad que por razón de su trabajo se le permita acceso, se le asignen derechos des uso y utilicen los recursos que componen los medios electrónicos de almacenamiento y transmisión de datos de Cesvi Colombia S.A.

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

Vulnerabilidad: Debilidad en la seguridad de la información de una organización, que potencialmente permite que una amenaza afecte a un activo; también puede ser la debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Work Place Cesvi Colombia: Es una red social de tipo empresarial, que pretende poner en contacto a todo el personal de Cesvi Colombia.

6. PLANTEAMIENTO ESTRATÉGICO

Cesvi Colombia S.A. establece que la información es vital para el desarrollo de sus actividades y cumplimiento de su Misión en razón a que es una herramienta fundamental para la toma de decisiones, motivo por el cual Cesvi Colombia está comprometido a proteger los activos de información de la entidad, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, la creación de cultura y conciencia de seguridad en los trabajador; tomando como base que la efectividad de esta política depende finalmente del comportamiento de las personas y los controles establecidos en las políticas de seguridad descritas en el presente documento.

La función de seguridad deberá asentarse sobre un conjunto de pilares, entendidos como aquellas características imprescindibles para conseguir una protección eficiente de la información de Cesvi Colombia S.A.

Dichas características son las siguientes:

- **La información aporta Valor:** proporcionando diferenciación y ventaja competitiva a la Compañía. Evolucionara en función de las necesidades corporativas a fin de mantenerse permanente integrada en el negocio, adaptándose a la estrategia corporativa.

- **La información es exacta:** la información a brindarse de ser suficientemente exacta para el grupo directivo, teniendo muy en cuenta cual es el propósito buscado.

- **La información es completa:** la información que será utilizada en la toma de decisiones debe estar disponible y debe informarnos acerca de los puntos clave del problema que se va a analizar y estudiar.

- **La información es integral para el conjunto de la Compañía:** afectara a todo el personal, a todos los medios e instalaciones y a todos los procesos y actividades de las diferentes unidades estratégicas de negocio y áreas de responsabilidad que involucren TI.

- **La información está orientada al servicio**: la función de seguridad tendrá una vocación de servicio a la organización, considerando a ésta, como su cliente y satisfaciendo las necesidades que desde la misma puedan ser demandadas.

- **Gestión de la información:** conjunto de procesos por los cuales se controla el ciclo de vida de la información, desde su obtención (por creación o captura), hasta su disposición final (su archivo histórico o eliminación). El objetivo de la gestión de la información es garantizar la integridad, disponibilidad y confidencialidad de la información.

- **Auto sostenibilidad:** con la actualización y mantenimiento diario de la información, garantizar su utilidad a futuro en todos los procesos que la demanden.

- **Política de confidencialidad del trabajador:** es el compromiso que adquiere cada trabajador de la compañía para utilizar y aprovechar de una manera adecuada la información de la misma.

- **Tratamiento de información de los clientes:** centralizada la información de las bases de datos de los clientes, garantizar el estricto cumplimiento de la ley.

- **Compromiso al interior:** Todos los usuarios de los sistemas de información y telecomunicaciones de Cesvi Colombia, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente manual.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad se elabora con el fin de proteger la información de la empresa, servirá además como guía para la implementación de medidas de seguridad que contribuyan a mantener la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas de información, redes y activos informáticos.

La Política de Seguridad de la información de Cesvi Colombia S.A. es el conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de la empresa, teniendo como propósito proteger la información, los recursos y la reputación de la misma.

El cumplimiento de la Política de Seguridad de la información de Cesvi Colombia S.A. es obligatorio y debe ser considerado como una condición en los contratos de personal.

La Política de Seguridad de la información de Cesvi Colombia S.A. centra su contenido en los siguientes pilares estratégicos:

- **El Software y los sistemas de información**: Todo software o sistema de información utilizado es de uso interno y solo para ser utilizado en tareas de la prestación del servicio y procesos organizacionales.

- **Confidencialidad de la información**: No se debe entregar datos o reproducir total o parcialmente la información generada por la entidad a personas ajenas o que no sean parte del proceso administrativo, comercial que legalmente corresponda.

- **Activos informáticos**: Cesvi Colombia es el dueño de la propiedad intelectual, de los avances tecnológicos e intelectuales desarrollados por sus trabajadores, derivados del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

- **Responsabilidad contractual con respecto a los equipos:** Cada trabajador será responsable por el mal uso del equipo de cómputo incluyendo daños en su sistema operativo por infecciones de virus, daño, pérdida o hurto.

- **Responsabilidad contractual con respecto a la Información:** Toda la información producida por los trabajadores de Cesvi Colombia S.A. incluyendo el correo electrónico es propiedad de la empresa, el trabajador no tiene ningún tipo de propiedad sobre la misma y en el momento de su retiro por cualquier causa la información debe ser entregada de forma clara, estructurada y completa.

8. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

8.1. Política de dispositivos móviles, planes celulares y de datos

Cesvi Colombia dentro de su política tiene establecido NO SUMINISTRAR teléfonos móviles/teléfonos inteligentes a sus trabajadores para el desarrollo de sus actividades; el alcance de la empresa llega hasta el suministro de la Simcard identificada con un número corporativo y cargada con un plan de minutos y datos mensuales; ambos limitados en tiempo y capacidad.

Nota: dependiendo del perfil y cargo del personal, este puede ser beneficiado con la entrega de una Simcard

Todos los números corporativos serán controlados y registrados por la Dirección de sistemas

8.2. Política de gestión de activos de información

Cesvi Colombia es propietario de los activos de información y los administradores de estos activos son los trabajadores (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información.

Los activos de TI serán gestionados bajo el HelpDesk corporativo Kwok Sys en la ruta www.cesvicolombia.com:300

8.3. Política de uso de los activos

Cesvi Colombia implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de los computadores personales corporativos o discos virtuales de red, archivos de video, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

Las directrices de uso de activos de información se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.1.

8.4. Política de uso de los de los computadores corporativos

Cesvi Colombia establece reglas que permitan orientar que la seguridad es parte integral de los activos de información y mediante la correcta utilización de los computadores corporativos por los usuarios finales.

Las directrices de uso de los computadores corporativos se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.2.

8.5. Política de uso de Internet

Cesvi Colombia permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso no adecuado de la información y las aplicaciones WEB.

La Dirección de Sistemas administrará la autorización de cambios a los permisos de navegación para los usuarios de Cesvi Colombia, previa solicitud del director de cada una de las UEN / ADR.

La Dirección de Sistemas implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los computadores corporativos, así mismo controla el acceso a la información contenida en portales de almacenamiento en Internet.

Los usuarios de los activos de información de Cesvi Colombia tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, plataforma de descargas de software, etc.; esto enmarcado en tres tipos de perfiles:

- Navega Normal
- Navega Sistemas
- Navega sin restricción

Los cuáles serán aplicados acorde a las funciones del cargo de cada usuario (director, coordinador, etc.). En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a la Dirección de Sistemas.

Las Directrices de uso de Internet se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.3.

8.6. Política de clasificación de la información

Cesvi Colombia consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado, define reglas de como clasificar la información por proceso y por año liderado por el proceso de Procesos, especificado en el documento PR-GC-002 Centro de Documentación-

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio ya sea magnético, papel, visual u otro que genere Cesvi Colombia como por ejemplo:
  - Formularios / comprobantes propios o de terceros
  - Información en los sistemas, equipos informáticos, medios magnéticos / electrónicos o medios físicos como papel
  - Otros soportes magnéticos / electrónicos removibles, movibles o fijos
  - Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación

- Los usuarios responsables de la información de Cesvi Colombia, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información puede ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo

- Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para Cesvi Colombia; independiente del tipo de activo, se deben considerar las siguientes características:

    - El activo de información es reconocido como valioso para Cesvi Colombia
    - No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores
    - Forma parte de la identidad de la organización y sin el cual Cesvi Colombia puede estar en algún nivel de riesgo
    - Los niveles de clasificación de la información valiosa que se ha establecido son: por proceso (UEN/ADR) y por año

Las reglas se encuentran definidas en el PR-GC-002 Centro de Documentación-

- Cesvi Colombia dispone de unidades de disco virtuales para los diferentes procesos con el fin de almacenar la información relevante definitiva de cada proceso. Es responsabilidad de los directores de UEN / ADR mantener ordenada y clasificada la información en esos discos virtuales

8.7. Política de control de acceso

Cesvi Colombia define las reglas para asegurar un acceso controlado, físico o lógico a la información y plataformas informáticas.

La conexión a la red de área local corporativa de Cesvi Colombia desde un sitio remoto, debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada por la Dirección de Sistemas.

Todo aplicativo informático o software debe ser comprado o aprobado por la Dirección de Sistemas.

Las reglas se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.4.

8.8. Política de establecimiento, uso y protección de claves de acceso

Ningún usuario deberá acceder a la red o a los servicios TIC de Cesvi Colombia, utilizando una cuenta de usuario o clave de otro usuario.

Cesvi Colombia suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados; las claves son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose con la Dirección de Sistemas.

Las contraseñas de acceso a la red corporativa deben tener mínimo 8 caracteres alfanuméricos, cada vez que se cambie esta debe ser distinta por lo menos de las últimas 3 anteriores.

La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ej: ¡”#$%)

8.9. Política de uso de discos de red o carpetas virtuales

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Las Directrices de uso de discos de red o carpetas virtuales se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.5.

8.10. Política de uso de puntos de red de datos (red de área local – LAN)

Asegurar la operación correcta y segura de los puntos de red.

Las Directrices de uso de puntos de red de datos, se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.6.

8.11. Política de uso de impresoras y del servicio de impresión

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Las Directrices de uso de impresoras y del servicio de impresión, se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.7.

8.12. Políticas de seguridad del centro de computo

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

En las instalaciones del centro de cómputo, No está permitido:

- Fumar al interior del centro de datos
- Introducir alimentos o bebidas
- El porte de armas de fuego, corto punzantes o similares
- Mover, desconectar y/o conectar equipos de cómputo sin autorización
- Modificar la configuración de los equipos o intentarlo sin autorización
- Alterar software instalado en los equipos sin autorización
- Alterar o dañar las conexiones físicas y/o eléctricas
- 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

Las Directrices de seguridad del centro de cómputo se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.8.

8.13. Políticas de seguridad de los equipos

Asegurar la protección de la información de los equipos de Cesvi Colombia.

Las Directrices de seguridad de los equipos se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.9.

8.14. Política de adquisición, desarrollo y mantenimiento de sistemas de información

Garantizar que la seguridad es parte integral de los sistemas de información.

Las Directrices de adquisición, desarrollo y mantenimiento de sistemas de información se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.10.

8.15. Política de respaldo y restauración de información

El objetivo es proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

Semanalmente la Dirección de Sistemas verificará la correcta ejecución de los procesos de Backup.

La Dirección de Sistemas debe generar tareas de restauración aleatorias de la información, estas tareas deben ser documentadas.

Las Directrices de los procesos de copias de seguridad se encuentran definidos en el documento DI-SI-001 Manual de criterios para copias de seguridad.

8.16. Política de seguridad de las comunicaciones

Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos y sistemas de comunicaciones.

Las Directrices de seguridad de las comunicaciones se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.11.

8.17. Política de uso del correo electrónico

Definir las pautas generales para asegurar una adecuada protección de la información de Cesvi Colombia, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

El personal de la Dirección de Sistemas no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Director de Sistemas.

Los usuarios y claves de acceso de los administradores de sistemas y del personal de la Dirección de Sistemas son de uso personal e intransferible.

El personal de la Dirección de Sistemas debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad.

Las Directrices de uso del correo electrónico se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.12.

8.18. Política de uso de mensajería instantánea y redes sociales

La Dirección de Sistemas define las pautas generales para asegurar una adecuada protección de la información de Cesvi Colombia, en el uso de los servicios de mensajería instantánea y de las redes sociales por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de internet, de cualquier trabajador de Cesvi Colombia, que sea creado a nombre personal en redes sociales como Twitter®, Facebook®, Youtube®, Likedink®, Instagram, etc, se considera fuera del alcance de la Política de Seguridad de la Información y por lo tanto su confiabilidad,

integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la Entidad debe ser autorizada por los Directores de área para ser socializadas y con un vocabulario e intención institucional.

No se debe utilizar el nombre de la Entidad en las redes sociales para difamar la imagen o reputación de los seguidores cuando responden comentarios en contra de la filosofía de la Empresa.

Las Directrices de uso de mensajería instantánea y redes sociales se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.13.

8.19. Política gestión de incidentes de TI

La Dirección de Sistemas de Cesvi Colombia pone a disposición de los usuarios una herramienta web que permite a los usuarios de la red corporativa reportar cualquier tipo de incidente a nivel de hardware, software o comunicaciones.

A todo trabajador la Dirección de Sistemas mediante acta o correo electrónico le asigna un usuario y contraseña para el ingreso al sistema HelpDesk ubicado en la URL (www.cesvicolombia.com:300).

El sistema permite generar reportes y exportarlos a diversas plataformas para desde allí realizar los análisis a que haya lugar, clasificando por cualquiera de las variables propias de cada ticket.

Las Directrices de uso del HelpDesk corporativo se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.14.

8.20. Política administración de usuarios SAP-BO

La Dirección de Sistemas define las pautas generales para asegurar una adecuada administración de las licencias del ERP corporativo SAP BO. El ERP es considerado como estratégico en la operación de Cesvi Colombia y por lo tanto el acceso, disponibilidad y control son fundamentales y de carácter prioritario para la Dirección de Sistemas.

Las Directrices de administración de usuarios SAP BO se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.15.

8.21. Política acceso a los servidores red corporativa

El acceso tanto físico como lógico a los servidores de la red corporativa de Cesvi Colombia es considerado como restringido y ningún trabajador podrá tener acceso directo a ellos salvo los consignados en este manual.

El acceso físico se rige por el capítulo 8.12. Políticas de seguridad del centro de cómputo y sus lineamientos.

Las Directrices de acceso lógico a los servidores red corporativa se encuentran definidas en el documento DI-SI-003 Lineamientos Política de Seguridad de la Información, numeral 3.16

9. ADMINISTRACIÓN DE LA SEGURIDAD

9.1. Gestión de cambios sistema SAP-BO

La administración del sistema SAP-BO está a cargo del ingeniero de soporte de sistemas, este cargo es el encargado de tramitar y dar solución a todos los requerimientos tanto propios como emitidos por los usuarios finales del sistema.

La empresa prestadora del servicio de consultoría para el ERP SAP-BO tiene implementado su propio protocolo para atender los requerimientos emitidos por sus clientes

Cuando un requerimiento es generado, se emite un número de ticket al cual el ingeniero de soporte le hace el seguimiento necesario hasta que el caso sea solucionado y se reciba a satisfacción la solución. El ticket es documentado con el fin de aportar los elementos necesarios para dar la trazabilidad a la solución.

A nivel interno, todo requerimiento debe estar soportado en un ticket interno del sistema HelpDesk de Cesvi Colombia S.A. www.cesvicolombia.com:300

No para todos los casos, pero si en contadas excepciones se hace necesario entregar la base de datos del sistema al proveedor de consultoría, esto con el fin de agilizar la solución a algún ticket. Esta entrega está sometida a los acuerdos de confidencialidad que se encuentran en los contratos suscritos entre Cesvi Colombia S.A. y el proveedor.

Todo requerimiento de cambios en la aplicación debe ser tramitado acorde al protocolo descrito previamente. Cuando existan requerimientos que involucren la intervención directa sobre la base de datos, el usuario debe diligenciar el requerimiento en sistema HelpDesk de Cesvi Colombia S.A. www.cesvicolombia.com:300 y soportarlo con el documento.

9.2. Segregación de ambientes de cómputo

Con el fin de garantizar la integridad de los datos de los ambientes de producción, se tienen diversos ambientes de pruebas para los sistemas que afectan de una u otra forma la información de la empresa.

Estos ambientes se forman básicamente con la réplica de la base de datos de producción y direccionando los programas para usar estas réplicas, garantizando así no afectar en ningún momento la información real.

Estos ambientes son utilizados con el fin de realizar pruebas sobre ajustes realizados a los sistemas de información, cambios de versiones o actualizaciones programadas.

Las bases de datos de los ambientes de pruebas están sujetas a protocolos de copias de seguridad no tan estrictos como las bases de datos de producción.

Las únicas personas con acceso a las bases de datos bien sean de producción o pruebas serán el Director de Sistemas como responsables de la administración general de los sistemas de información y servidores de la compañía y el ingeniero de soporte de sistemas como responsable de la administración de varios de los sistemas de información de Cesvi Colombia.

9.3. Gestión de copias de seguridad

La gestión de las copias de seguridad se encuentra definida en el documento DI-SI-001 Manual de criterios para copias de seguridad.

9.4. Gestión de Jobs y Scripts

Cesvi Colombia S.A. para el desarrollo de sus consultas, actualizaciones, y tareas programadas sobre sus bases datos que involucran la información financiera, ha desarrollado una serie de Jobs y Scripts.

Para llevar un control de estos Jobs y Scripts, se cuenta con dos archivos en los cuales se registra la información detallada de cada uno de ellos, los archivos son:

- Gestión Job-Script SAP-BO.xlsx

El control de estos archivos es responsabilidad del Director de Sistemas y el registro de modificaciones, actualización o inclusión de nuevos Jobs o scripts a cargo del ingeniero de soporte de sistemas.

9.5. Gestión de Licenciamiento

La Dirección de sistemas tiene implementado en el acta de entrega de los equipos de cómputo un anexo de responsabilidad que dice:

"Anexo de Responsabilidad

El usuario a quien se entrega este equipo, se hace responsable en su totalidad por el Software que posterior a la entrega sea instalado, se compromete a asumir las responsabilidad legal y penal ante cualquier hecho de piratería o uso de software no autorizado por Cesvi Colombia S.A.

De requerir algún Software adicional debe ser consultado con el proceso de Sistemas sobre la disponibilidad de Licencias."

El acta de entrega se anexa al historial del equipo de cómputo en el sistema HelpDesk en el módulo de hardware.