1. OBJETIVO

Establecer las normativas y políticas para el uso, control y administración de las Tecnología de Información y Comunicaciones que deben conocer y cumplir todos los funcionarios de Vigilancia y Seguridad Limitada (en adelante VISE).

2. ALCANCE

Estas políticas son aplicables y efectivas para todos los funcionarios y contratistas de VISE que utilicen sus servicios e infraestructura de tecnología y comunicaciones.

Los dispositivos regulados y atendidos por estas políticas son:

- Aquellos que hacen parte de los activos fijos de VISE.
- Aquellos de propiedad de terceros que usan servicios o la infraestructura de VISE

3. DEFINICIONES

3.1. **TIC:** Tecnologías de la Información y Comunicaciones

3.2. **Servidor:** Es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

3.3. **Centro de Cómputo:** Es el lugar donde se alojan los servidores y equipos de comunicación necesarios para la operación de las actividades informáticas de VISE.

3.4. **Dispositivos:** Todos aquellos equipos como computadores, tablets, Smartphone, etc. que son utilizados para almacenamiento, procesamiento y comunicación de datos.

4. RESPONSABLE

El responsable del direccionamiento y ejecución del procedimiento es el Director de Sistemas.

5. CONTENIDO

5.1 Políticas

5.1.1 Políticas Generales

- Bajo ninguna circunstancia los colaboradores de la empresa, pueden utilizar los recursos informáticos para realizar actividades prohibidas por las normas establecidas o por normas jurídicas nacionales o internacionales.

- Todos los equipos de cómputo y portátiles propiedad de VISE deben ser vinculados al dominio corporativo “viseltda.com.co” y se rigen bajo los parámetros y normas de seguridad definidas en el servidor de dominio, se exceptúan aquellos equipos que físicamente se encuentran de manera permanente fuera de las instalaciones principales de VISE en Bogotá.

- Todos los dispositivos propiedad de VISE o de Terceros que usan o comparten servicios o recursos de infraestructura se acogen a los parámetros y normas de seguridad definidos en los diferentes sistemas de control de la compañía.

- Los equipos propiedad de VISE, solo pueden ser intervenidos por el departamento de Sistemas; su personal es el único autorizado para realizar las actividades de soporte técnico y cambios de configuración en el equipo de cómputo. En el caso de labores de mantenimiento efectuadas por terceros éstas deben ser previamente aprobadas la Dirección de Sistemas.

- VISE y su departamento de sistemas no tienen ningún alcance y responsabilidad de soporte frente a equipos de terceros, salvo la supervisión de las condiciones mínimas de seguridad para la vinculación a sus servicios o infraestructura, en todo caso se requiere la autorización del Director de Sistemas.

- En cumplimiento con normativas de seguridad y sistemas de gestión los usuarios vinculados al dominio exigen el cambio de contraseña cada 45 días.

5.1.2. Adquisición de Hardware, Software y Tecnología

- La adquisición, compra o arrendamiento de todo tipo de equipos de cómputo, periféricos, hardware en general y software debe contar con el Vo.Bo. del área de Sistemas, salvo aquellos recursos destinados a servicios o contratos propios del área de la Gerencia de Tecnología quien se hace responsable de este inventario y licenciamiento respectivo cuando corresponda.

- La compra de servicios como nombres de dominio, hosting, todo tipo de servicios o aplicaciones en la nube debe ser tramitado con el área de Sistemas, la cual gestionará y administrará estos recursos.

5.1.3. Uso de Equipos de Computo

- Todo equipo de cómputo, propiedad de VISE, deberá ser utilizado únicamente para actividades relacionadas con los objetivos y metas de la empresa.

- El área de Sistemas deberá implementar las acciones necesarias para el correcto funcionamiento de los equipos de cómputo, tales como actividades preventivas consideradas en el plan de mantenimiento.

- La solicitud de repuestos, componentes, periféricos y/o accesorios de equipo de cómputo debe ser tramitado a través del departamento de sistemas mediante su mesa de ayuda.

- Para conectar una computadora a la red institucional que no esté bajo el control administrativo de VISE (computadoras privadas del personal, computadoras de otras empresas o terceros en general, las cuales no están sujetas a la totalidad de las políticas de seguridad de VISE y por ende constituyen un riesgo al ser conectadas a la red institucional) se deberá solicitar permiso al área de Sistemas para que ésta inspeccione el equipo, compruebe que no constituye un riesgo para la seguridad y brinde la autorización respectiva.

- Cuando exista algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa a un equipo de cómputo de VISE, deberá ser notificado de inmediato al área de Sistemas.

- Sólo el personal autorizado por el área de Sistemas está facultado para abrir o intervenir físicamente los equipos de cómputo propiedad de VISE.

- Todos los equipos de cómputo bajo la supervisión de VISE, deben contar con un software antivirus actualizado, con el objetivo de proteger el equipo de programas maliciosos.

- Todos los equipos de cómputo bajo la supervisión de VISE, son periódicamente actualizados con los parches de seguridad pertinentes para el sistema operativo y aplicaciones.

- Todas las computadoras conectadas a la red VISE contarán obligatoriamente con un fondo o tapiz definido por el área de Sistemas a fin de preservar la imagen corporativa.

5.1.4. Centro de Cómputo

- El acceso al centro de cómputo es restringido y sólo personal autorizado por el área de Sistemas puede tener acceso a él.

- Sólo el personal autorizado por el área de Sistemas puede abrir los gabinetes, servidores y equipos al interior del centro de cómputo o racks de distribución.

- El acceso a los servidores de VISE, ya sea usando consola de administración local o una consola de administración remota es restringido a personal autorizado por el área de Sistemas. El intento de conexión por alguna persona no autorizada a cualquier consola de administración de los servidores se considera una violación de las políticas de seguridad y está sujeto a las medidas disciplinarias que corresponda.

5.1.5. Propiedad de la Información

- Todos los datos que los funcionarios de VISE crean y manipulan en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico, durante el desarrollo normal de sus actividades laborales, son propiedad de VISE.

- Los derechos patrimoniales de un programa de computación, hojas de cálculo, archivos de Word, macros, etc. y su documentación, creados por uno o varios funcionarios en el ejercicio de sus actividades laborales corresponden a VISE.

- Toda copia de seguridad o Backup que contenga información de VISE, realizada bajo responsabilidad del usuario, debe ser entregada al momento de la finalización de la relación laboral.

- Todo funcionario que tenga contacto con la información de la organización en cualquier formato o con cualquier servicio de procesamiento de información, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la misma, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial.

5.1.6. Actividades Prohibidas

- Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.

- La distribución o instalación de software sin la licencia de uso adquirida por VISE (ver numeral 5.1.11.).

- Difundir información identificada como confidencial a través de medios que involucren el uso de la Tecnología de Información.

- Introducir software malicioso en la red o en los servidores (virus, worms, envío masivo de correo electrónico, etc.)

- Utilizar la infraestructura de tecnología de información de VISE para conseguir o transmitir material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de

comunicaciones de VISE con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.

- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de VISE.

- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.

- Monitorear puertos o realizar análisis del tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad. El personal del área de Sistemas, es responsable de la Seguridad Informática y puede realizar estas actividades siempre y cuando sean previamente autorizadas por la dirección del departamento.

- Ejecutar cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada.

- Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

- Interferir o negar servicios previamente autorizados por VISE.

- Usar comandos o programas para el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet, Intranet).

- Modificar la configuración de sistemas operativos, aplicativos institucionales (sistemas ERP, reporteadores, etc.), software antivirus, firewall personales o políticas de seguridad en general implantadas en los equipos de cómputo de VISE sin consultar previamente con el área de Sistemas, la cual analizará la viabilidad de los cambios solicitados.

- Descargar archivos de gran tamaño que puedan afectar los canales de datos y comunicación de las compañías.

- Excepciones: Para propósitos de mantenimiento de la red y de seguridad los funcionarios del área de Sistemas, pueden estar exentos de seguir algunas de las restricciones anteriores, debido a las responsabilidades de su cargo o a eventos programados. Estas actividades deben ser programadas y previamente autorizadas por el director de sistemas.

5.1.7. Manejo de Contraseñas

El cumplimiento de la política de contraseñas por parte de los usuarios es de vital importancia ya que éstas constituyen la primera línea de defensa para garantizar que la información sólo sea accedida por el personal autorizado. No existe ninguna tecnología

que pueda prevenir el acceso no autorizado, atribuible a causales del uso indebido de las contraseñas.

- Todos los usuarios internos de VISE requieren de un nombre de usuario y una contraseña para utilizar el equipo de cómputo asignado y acceder a los servicios de redes en la compañía.

- Las contraseñas de los usuarios deben cumplir los siguientes requisitos de seguridad: tener un mínimo de ocho (8) caracteres alfanuméricos, contener una letra mayúscula, un número y un carácter especial.

- Las contraseñas son personales, intransferibles y conocidas únicamente por el propio usuario el cual será responsable de toda la actividad que se realice con ella.

- El área de sistemas se reserva el derecho de restablecer en cualquier momento la contraseña de cualquiera de los usuarios de VISE, con previo aviso para no afectar de ninguna manera la continuidad de su trabajo, si se detecta que ésta ha sido comprometida.

- Todas las computadoras de escritorio y portátiles asociados al dominio son bloqueados de manera automática después de 5 minutos de inactividad, el equipo está nuevamente disponible tras el ingreso de la clave del usuario.

- La configuración de los usuarios de los equipos localizados en las sucursales son responsabilidad del área de sistemas y sólo ésta tiene la autoridad para realizar cambios de configuración a dichos equipos.

- Prohibiciones: 1) Revelar la contraseña personal o permitir su uso a terceros para actividades ajenas a la misión de VISE, la prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario, cuando la conexión a la red VISE se realice desde el hogar. 2) Anotar la contraseña en libretas o cualquier otro medio físico y tenerla a la vista de todos en su lugar de trabajo. Se recomienda que la contraseña sea aprendida de memoria y no anotarla en ningún medio físico como libretas, cuadernos etc.

5.1.8. Correo Electrónico

- La comunicación institucional realizada por Correo Electrónico, solo será a través de las cuentas asignadas.

- El Correo Electrónico es correspondencia privada entre el emisor y el destinatario, por lo tanto, no podrá trasmitirse a través de Internet información considerada como de uso confidencial hacia el personal externo de VISE, salvo la información considerada como parte de la gestión operativa y comercial.

- El usuario es responsable del contenido de los mensajes enviados esto incluye entre otros: Contenido de material ofensivo u obsceno, cualquier quebrantamiento de propiedad intelectual, copyright o cualquier información ilegal o criminal.

- Se prohíbe la transmisión de mensajes que puedan: Crear un medio hostil sobre la raza, edad, sexo, religión, política, nacionalidad, origen, incapacidad u orientaciones personales; comentarios despectivos, noticias informales o mal intencionadas, cadenas de cartas, mensajes masivos de índole personal, y en general cualquier tipo de información que cause congestión en la red o interfiera con el trabajo de otros.

- El área de Sistemas bloqueará en forma automática la recepción de correos electrónicos desde aquellas direcciones que se han identificado como fuentes de correo Spam, virus y código malicioso en general. En caso que el usuario necesite recibir correo electrónico desde alguna de estas direcciones identificadas como ofensivas debe comunicarse con el área de Sistemas para analizar el caso y atender su solicitud.

- Dado que los recursos de almacenamiento y redes son limitados los buzones han sido limitados en su capacidad de almacenamiento a 2GB por buzón y tamaño de archivos adjuntos a 10MB.

5.1.9. Internet

- Los funcionarios son responsables de mantener su imagen profesional dentro de Internet, así como proteger la imagen y reputación de VISE.

- Solo está permitido acceder a los servicios de Internet por los medios físicos dispuestos por la el área de Sistemas: 1) cuando el equipo se encuentre conectado a la red local dentro de las instalaciones de la compañía. 2) para el caso de los equipos portátiles cuando se encuentran fuera de la compañía podrán conectarse a Internet por los medios disponibles en cada momento, sin embargo, el intercambio de información con la red local será únicamente a través de una conexión privada virtual en el caso de los usuarios autorizados para este servicio.

- No se debe de utilizar el acceso a Internet como un medio de participación, acceso y distribución de actividades o materiales que vayan en contra de la Ley o las políticas de la compañía.

- No se autoriza acceder, ver o bajar desde sitios de Internet: gráficos, imágenes o cualquier otro material que pueda ser percibido como obsceno, abusivo o que contenga humor inapropiado, lenguaje amenazante, acosante u otra forma de lenguaje objetable dirigido a un individuo o grupo.

- El área de Sistemas asignará a cada usuario con acceso a Internet un perfil de navegación en concordancia con sus actividades y funciones. Como resultado de

esto el usuario tendrá bloqueado automáticamente las páginas con contenido ofensivo, malicioso o de carácter personal como redes sociales.

5.1.10. Almacenamiento y Copias de Seguridad

- La información obtenida de cualquiera de los servicios internos deberá ser almacenada localmente en el equipo de cómputo del usuario y no puede ser distribuida o transmitida por la red institucional, sin la autorización respectiva.

- Las áreas de almacenamiento en la Red (púbico y digitalización) deben ser tratadas como almacenamientos temporales y su uso está restringido a documentos. El área de Sistemas revisará el aprovechamiento óptimo de los recursos compartidos para mantener la integridad y para asegurar que los usuarios utilicen los recursos de manera responsable. Sobre estas ubicaciones se generan copias de seguridad diarias como parte de los controles y cumplimiento de las políticas internas.

- Las unidades de red de usuario, deben mantener estrictamente la información requerida para el trabajo diario, todo dato con antigüedad superior de 12 meses debe ser archivado en backup mediante solicitud al departamento de sistemas a través de la mesa de ayuda.

- Todo dispositivo de almacenamiento externo conectado a un equipo de la compañía debe ser analizado por el software antivirus antes de su uso.

- Todos los usuarios deben acogerse y facilitar el proceso de backup de información de acuerdo con el cronograma establecido, bajo ninguna circunstancia y bajo responsabilidad propia del usuario, no se debe permitir que transcurran más de 90 días sin copia de seguridad bajo la custodia del área de Sistemas. Todo proceso de backup es registrado en el formato GTST0501.03 Control para la Toma de Copias de Respaldo o Backups.

- Cada usuario debe según la necesidad auto archivar o mover el correo electrónico antiguo a la bandeja “Histórico” para la generación del backup respectivo y liberación de espacio de su buzón. (Ver GAST0402 Instructivo Autoarchivado de Correo Electrónico)

5.1.11. Propiedad y Derechos de Contenidos

- La información disponible en Internet, incluyendo textos, software, música, sonido, fotografía, video, gráficos u otro material, está protegida por copyright, marcas registradas, patentes u otros derechos de propiedad y leyes. Sólo se permite el uso de este material bajo autorización expresa del autor (Ley 44 de 1993).
- Los usuarios no deben descargar ni instalar ningún tipo de software comercial, shareware o freeware en los equipos de trabajo, de ser necesario se debe tramitar a través del área de Sistemas.

5.1.12. Conducta del usuario

- El usuario es el único responsable del contenido de transmisiones a través de cualquier servicio.
- El usuario debe cumplir con las leyes de transmisión de datos técnicos de los países desde los cuales y hacia donde se envían los mensajes de Correo Electrónico.
- El usuario no debe usar el servicio para propósitos ilegales o de entretenimiento.
- El usuario debe cumplir con todas las regulaciones, políticas y procedimientos internos.
- La comunicación de los usuarios se debe conducir con respeto y consideración, evitando los abusos y el uso del lenguaje inapropiado.
- Se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades propias del trabajo y funciones del colaborador.

5.1.13. Administración de Software

El área de Sistemas, es la única área autorizada para llevar a cabo la administración del software de VISE, por lo que dentro de sus responsabilidades tiene:

- Mantener bajo resguardo las licencias de uso de software.
- Llevar un control de las licencias en operación y el equipo en el cual se encuentra en uso, salvo aquellas asociadas a proyectos de la Gerencia de Tecnología.
- Organizar la inspección de equipos de cómputo en intervalos regulares.
- Difundir a los empleados las Políticas de Uso de Software con el fin de que conozcan la normatividad en este concepto.
- Realizar un análisis de necesidades y requerimientos de software para su adquisición o actualización.

5.1.14. Instalación y Soporte de Software

- El área de Sistemas es la única autorizada, así como responsable de realizar la instalación de software y proporcionar soporte del mismo en todos los equipos de cómputo.

- Se prohíbe la instalación de copias ilegales de cualquier programa descargado de Internet, software adquirido para uso personal del usuario o software de esparcimiento.

5.1.15. Proveedores de Servicio y Niveles SLAs (Acuerdo de Nivel de Servicio)

- El departamento de sistemas debe identificar los servicios y equipos críticos de su responsabilidad.

- VISE debe contar con proveedores de soporte para servicios y equipos críticos con personal especializado y soporte 24x7 con un máximo de 4 horas de respuesta en sitio para eventos críticos.

5.1.16. Ventanas de Mantenimiento con Afectación de Servicios

- Todo evento de mantenimiento o intervención preventiva o correctiva que impacte en la continuidad de los servicios de correo electrónico, canales de internet o aplicaciones internas debe ser programado con mínimo 5 días hábiles de anticipación en coordinación con el área de monitoreo para conciliar fecha y hora con menor impacto en la operación.

- Las emergencias, imprevistos o no controlables por el personal del área de sistemas serán atendidas con el criterio de urgencia por el personal interno, de igual manera se activarán los escalamientos de SLAs con los proveedores que corresponda para solucionar los incidentes en el menor tiempo posible.

6. RESPONSABILIDADES

6.1. El área de Sistemas es la responsable del seguimiento y administración de las políticas de Tecnología de Información y Comunicaciones.

6.2. El área de Sistemas es la responsable de la asignación y distribución de los equipos de cómputo.

6.3. El área de Sistemas es la responsable de la administración y asignación de los servicios informáticos de la compañía.

6.4. Cada usuario de uno o varios de los servicios TIC o con asignación de equipos es responsable de cumplir los procedimientos internos y las políticas de control y seguridad.

6.5. Es responsabilidad del área de Sistemas, elaborar y ejecutar anualmente un plan de mantenimiento preventivo.

6.6. Son responsabilidades del usuario:

- Administrar las cuentas y claves de acceso hacia los diferentes servicios y sistemas internos.

- Notificar inmediatamente al área de Sistemas cualquier uso no autorizado de su cuenta, o cualquier intrusión de seguridad conocida.

- Usar los servicios con fines institucionales.

- Analizar cualquier archivo o programa obtenido a través de Internet o Correo Electrónico con software antivirus.

- Realizar las descargas habituales del correo, para evitar que los buzones se saturen, ya que el espacio en el servidor de correo es limitado.

- No utilizar el Correo Electrónico corporativo en suscripciones a listas que saturen la capacidad de almacenamiento del buzón o para fines personales.

- Cambiar las contraseñas para ingreso a los sistemas cada 45 días, cuando éstos no exijan el cambio de manera automática.

7. LINEAMIENTOS GENERALES

7.1. Uso Adecuado de las TIC

Las políticas definidas en este documento están relacionadas con los equipos de cómputo que son asignados a los usuarios, el centro de datos, aspectos relacionados con la propiedad de la información que es creada y manipulada por los usuarios y la utilización de los recursos informáticos que la empresa pone a disposición de sus colaboradores para que desarrollen sus actividades.

7.2. Seguridad Informática y de la Información

La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

7.3. Internet y Correo Electrónico

Los servicios de Acceso a Internet y Correo Electrónico son administrados institucionalmente por el área de Sistemas, quien tomará los reportes de los problemas

técnicos y errores de recepción y envío relacionados con los servidores, para su posible atención inmediata. Sin embargo, el (los) proveedor(es) del enlace principal a Internet es responsable de garantizar la disponibilidad del servicio y los servicios contingentes contratados.

7.4. Los servicios de tecnología pueden verse afectados durante la ejecución de las actividades de mantenimiento programadas y ante fallas eventuales cuya intervención puede implicar la baja de uno o varios servicios.

8. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
No DE CAMBIO	**DESCRIPCIÓN**	**FECHA**
00	Primera Edición	09/04/2015

9. CONTROL DE REGISTROS

N/A

Código	**Identificación**	**Almacenamiento**		**Tiempo de Almacenamiento**	**Recuperación**	**Disposición**
		Sitio	**Carpeta**			