POLÍTICAS	FECHA DE ELABORACIÓN	PÁGINA
	ENERO– 2019	1 de 43
	CÓDIGO	VERSIÓN
	GTIC-DRS-003	02

POLÍTICAS DE SEGURIDAD DE DATOS E INFORMACIÓN

GERENCIA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

HOJA DE REVISIÓN Y APROBACION

Por medio de la presente se certifica que este manual ha sido revisado, avalado y aprobado por las unidades responsables que intervienen en el proceso y entrara en vigencia cuando sea aprobado por la Junta Directiva de la C.A. Venezolana de Televisión.

GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO			
ELABORADO POR:	**REVISADO Y AVALADO POR:**		
Analista	**Coordinación de Organización y Procesos**	**Coordinación de Sistemas y Procesos**	**División de Planificación**
Aileen Gamardo	Alba Sanabria	Noemí Pinto	Lubins Porras
APROBADO POR:			
Gerencia de Planificación y Presupuesto		**Gerencia Tecnología de la Información y Comunicación**	
Paul Pérez		Ivan Quiroz	
Consultoría Jurídica		**Vicepresidencia Ejecutiva**	
Omaira Alzuarde		Paola Gómez	

ELABORADO POR:	REVISADO POR: COORDINACIÓN DE ORGANIZACIÓN Y PROCESOS/ SISTEMAS Y PROCESOS	REVISADO POR: DIVISIÓN DE PLANIFICACIÓN	APROBADO POR: GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO	APROBADO POR: GERENCIA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Aileern Gamardo	**Alba Sanabria/** Noemi Pinto	**Lubins Porras**	**Paúl Pérez**	**Ivan Quiroz**

POLÍTICAS DE SEGURIDAD DE DATOS E INFORMACIÓN	FECHA DE ELABORACIÓN	PÁGINA
	ENERO- 2019	3 de 43
	CÓDIGO	VERSIÓN
	GTIC-DRS-003	02

POLÍTICAS DE SEGURIDAD DE DATOS E INFORMACIÓN	FECHA DE ELABORACIÓN	PÁGINA
	ENERO- 2019	4 de 43
	CÓDIGO	VERSIÓN
	GTIC-DRS-003	02

OBJETIVO

Dotar de la información necesaria en el más amplio nivel de detalle a los usuarios, trabajadores y personal ejecutivo de la C.A. Venezolana de Televisión en las políticas, normas y mecanismos que se deben cumplir para proteger el hardware y software de la red institucional, así como la información que es procesada y almacenada en estos.

ALCANCE

Las políticas contempladas en este manual, deben ser acatadas por todos los trabajadores de la C.A Venezolana de Televisión, como mecanismo de control interno para salvaguardar todos los recursos tecnológicos tanto Software como Hardware.

UNIDADES QUE INTERVIENEN

- Vicepresidencia de Soporte Tecnológico.
- Gerencia Tecnología de la Información y Comunicación.
- Unidades organizativas de la C.A. Venezolana de Televisión.

TÉRMINOS UTILIZADOS

Términos	Descripción
Activo	Conjunto de bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la C.A. VTV.
Administración Remota	Forma de administrar los equipos informáticos o servicios de la C.A. VTV a través de equipos o equipos remotos, físicamente separados del usuario final.
Amenaza	Es un evento que puede desencadenar un incidente en la empresa, produciendo daños materiales o pérdidas inmateriales en sus activos.
Archivo Log	Ficheros de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, equipos o IP´s involucradas en el proceso, entre otros).
Ataque	Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
Confidencialidad	Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.
Cuenta	Mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.
Desastre o Contingencia	Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Disponibilidad	Los recursos de información sean accesibles, cuando estos sean necesitados.
Encriptación	Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.
Integridad	Proteger la información de alteraciones no autorizadas por la Empresa.
Impacto	Consecuencia de la materialización de una amenaza.
Políticas de seguridad	Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la Empresa. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una Empresa previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.
Outsourcing	Contrato por servicios a terceros, tipo de servicio prestado por personal de empresa externa, ajeno a la C.A. VTV.
Responsabilidad	En términos de seguridad, significa determinar que individuo en la C.A. VTV, es responsable directo de mantener seguros los activos de cómputo e información.
Servicio	Conjunto de aplicativos o programas informáticos, que apoyan la labor administrativa, sobre los procesos diarios que demanden información o comunicación de la C.A. VTV.
SGSI	Sistema de Gestión de Seguridad de la Información.
Soporte Técnico	Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la C.A. VTV.
Riesgo	Posibilidad de que se produzca un impacto determinado en un activo, dominio o en toda la Empresa.

Terceros	Proveedores de software, que tengan convenios o profesionales con la C.A. VTV.
Sistemas de Alimentación Ininterrumpida (SAI) o UPS	Sistemas de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (**UPS**), es un dispositivo que utiliza baterías u otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.
Usuario	Defínase a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga una especie de vinculación con la Empresa.
Vulnerabilidad	Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

MARCO LEGAL

- Constitución de la República Bolivariana de Venezuela, publicada Gaceta Oficial Extraordinaria de la República Bolivariana de Venezuela Nº 5.453 de fecha 24-03-2000.
- Ley Orgánica de Telecomunicaciones de 1 de junio de 2000 (Gaceta Oficial de la República Bolivariana de Venezuela Nº 36.970 de 12 de junio de 2000).
- Ley 48 de 4 de septiembre de 2001. Especial contra Delitos Informáticos (Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.313 de 30 de octubre 2001).
- Decreto 825 del 10 de mayo de 2000 sobre Internet como prioridad de la República Bolivariana de Venezuela. (Publicado en Gaceta Oficial de la República Bolivariana de Venezuela Nº 36.955 del 22 de mayo de 2000).
- Decreto con Fuerza de Ley 1.204 sobre Mensajes de Datos y Firmas Electrónicas del 10 de febrero de 2001. (Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 del 28 de febrero de 2001).
- Decreto N° 3.335 de 12 de diciembre de 2004. Reglamento parcial del Decreto Ley sobre mensajes de datos y firmas electrónicas (Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.086 del 14 de diciembre de 2004).
- Decreto Nº 3.390 de 23 de diciembre de 2004 sobre software libre. (Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.095 de 28 de diciembre de 2004).
- Resolución 240 del Ministerio de Ciencia y Tecnología del 9 de noviembre de 2004, por la que se crea el Nombre de Dominio: gov.ve.

POLÍTICAS

Criterios:

1. Del Desarrollo de Software.

1.1. Los sistemas automatizados de información de la C.A. Venezolana de Televisión, deben ser diseñados bajo metodologías de desarrollo que permitan definir el alcance y delimitación de cada fase del proyecto, incorporando en los mismos, controles preventivos tales como: perfiles de auditoría sobre los procedimientos que permitan visualizar a los usuarios que interactúan con dicho sistema, además de contar entre otros aspectos con los procesos de prueba y aprobación del mismo.

1.2. Todo software desarrollado dentro de la empresa que tenga el objetivo de procesar información sensible, valiosa o crítica debe contener la documentación con las especificaciones necesarias para el desarrollo del modelo conceptual del sistema, así mismo, queda prohibido desarrollar software en cualquier unidad diferente a la Gerencia Tecnología de la Información y Comunicación, cuya documentación es competencia de la División de Planificación adscrita a la Gerencia de Planificación y Presupuesto.

1.3. Los sistemas de información de la C.A. Venezolana de Televisión, deben pasar al ambiente de producción, una vez que se efectúen las pruebas requeridas que evidencien la excelente funcionalidad técnica del mismo en el ambiente de desarrollo, correspondiendo a los usuarios involucrados, evaluar y otorgar el visto bueno, así como al grupo multidisciplinario que se designe para la evaluación del proyecto.

1.4. Los programadores, asesores y empresas (outsourcing) que hayan estado involucrados en el desarrollo de alguna aplicación específica, no deben formar parte de las evaluaciones formales o de la operación en producción día a día del sistema, unicamente deben servir de apoyo para ejecutar las pruebas que sólo podrán realizar los usuarios directos.

2. De la adquisición de Hardware y Software:

2.1. Todo hardware y software, debe ser evaluado por la Gerencia Tecnología de la Información y Comunicación, en el caso particular donde dichas herramientas sean específicas para una

unidad, serán la Gerencia Tecnología de la Información y Comunicación y la Unidades Solicitante del recurso las responsable de su evaluación y aprobación antes de ser adquiridos por la C.A. Venezolana de Televisión, además de verificar que posean las licencias y programas fuentes respectivos, quedando estos debidamente documentados en el contrato y descartando futuras dependencias con empresa alguna.

2.2. Toda adquisición de hardware y software, debe estar basada en los requerimientos con los que deben cumplir los productos, por lo tanto para el proceso de adquisición se diseñan los parámetros de selección (matriz de evaluación) que permitan medir sus bondades y su compatibilidad con la plataforma tecnológica de la C.A. Venezolana de Televisión.

2.3. Todos los sistemas de información de la C.A. Venezolana de Televisión, deben especificar los requerimientos de seguridad necesarios, de acuerdo a los estándares definidos por la empresa, evaluando las alternativas con los proveedores, para que exista un adecuado balance entre seguridad y otras características como: facilidad de uso, simplicidad operacional, actualizaciones, costos aceptables, además que se reflejen los siguientes aspectos tecnológicos:

2.3.1. De Seguridad de Datos: medir y determinar el grado de recuperación y auditabilidad de los datos y operatividad de los sistemas.

2.3.2. Aspectos administrativos: para dejar claro las condiciones contractuales y de servicio por parte de las empresas oferentes.

2.3.3. Aspectos funcionales: ponderar el grado de aceptación por parte del usuario en cuanto a la satisfacción de las necesidades operativas y funcionales que el sistema les ofrece.

Políticas de Seguridad Informática.

Nivel 1: Seguridad Organizativa.

1. Políticas de Seguridad.

1.1. La C.A. Venezolana de Televisión reconoce que un elemento para cumplir con su misión y alcanzar sus objetivos, debe garantizar la confidencialidad, integridad y disponibilidad de toda la información y recurso informático de su propiedad, bajo su administración o custodia.

1.2. Toda información desarrollada o generada por los trabajadores o personal contratado por la empresa, es propiedad de la misma y no puede ser obsequiada, transferida, ni utilizada para, beneficio personal o de terceros.

1.3. Ningún trabajador, indistintamente de su jerarquía, así como el personal contratado o cualquiera que realice algún trabajo en la empresa, podrá divulgar la información que es propiedad de la C.A. Venezolana de Televisión.

1.4. El incumplimiento de estas políticas trae como consecuencia la aplicación de acciones correctivas y medidas disciplinarias, así como también, sanciones legales de acuerdo al hecho ocurrido y a lo expuesto en la Ley Especial Contra los Delitos Informáticos.

1.5. Los servicios de red de la C.A. Venezolana de Televisión son de exclusivo uso para generar información y programas en el ámbito cultural, deportivo, noticioso, político, de investigación, técnicos y gestión administrativa, cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento.

1.6. La Presidencia Ejecutiva de la C.A. Venezolana de Televisión, delega en la Gerencia Tecnología de la Información y Comunicación el seguimiento del cumplimiento de la normativa y propicie el entorno necesario para crear un sistema de gestión de seguridad de la información (SGSI), el cual tendrá entre sus funciones:

- Velar por la seguridad de los activos informáticos
- Gestión y procesamiento de información.
- Cumplimiento de políticas.
- Elaboración de planes de seguridad.
- Capacitación de usuarios en temas de seguridad informática.
- Gestionar y coordinar esfuerzos, para crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad dentro de la empresa. El mismo, sirve de guía a los trabajadores por medio de métodos necesarios para aplicar ante cualquier eventualidad que se presente.
- Informar sobre problemas de seguridad a la alta gerencia.
- Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

1.7. El titular de cada unidad dentro de la red institucional es el único responsable de las actividades procedentes de sus acciones.

1.8. Todo usuario de la red institucional de la C.A. VTV, tiene absoluta privacidad sobre su información o la proveniente de sus acciones, Excepto en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional, sus servicios o cualquier otra red ajena a este canal.

1.9. Los usuarios tendrán el acceso a Internet, siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad de informática.

2. Excepciones de Responsabilidad.

2.1. Los usuarios que por disposición de sus superiores realicen acciones que perjudiquen a otros usuarios o la información que estos procesan, y no cuentan con un contrato de confidencialidad y de protección de la información de la empresa o sus allegados.

2.2. Los usuarios pueden estar exentos de responsabilidad, o de seguir algunas de las políticas enumeradas en este documento por la responsabilidad de su cargo, o a situaciones no programadas. Estas excepciones, debe ser solicitadas formalmente y aprobadas por la Gerencia Tecnología de la Información y Comunicación, con la documentación necesaria para el caso, siendo la gerencia responsable de su aprobación final.

3. Clasificación y Control de Activos.

a) Responsabilidad por los activos:

3.1. Cada unidad, tiene un responsable por el (los) activo(s) crítico(s) o de mayor importancia para la empresa.

3.2. El titular responsable de los activos de cada unidad, debe velar por la salvaguarda de los activos físicos (hardware y medios magnéticos, aires acondicionados, mobiliario, u otros), activos de información (Bases de datos, archivos, documentación de sistemas, procedimientos operativos, configuraciones) y activos de software (aplicaciones, software de sistemas, herramientas y programas de desarrollo).

3.3. La Gerencia Tecnología de la Información y Comunicación, es responsable de la seguridad de la información almacenada en esos recursos.

b) Clasificación de la información:

3.4. De forma individual: los supervisores de cada unidad tienen la responsabilidad de clasificar de acuerdo al nivel de importancia, la información que en ella se procese.

3.5. En base a criterios:

- Pública.
- Interna.
- Confidencial.

3.6. Los activos de información de mayor importancia para la C.A. VTV, debe clasificarse por su nivel de exposición o vulnerabilidad.

4. Seguridad Ligada al Personal:

Referente a personal contratado:

4.1. Se entrega al contratado, toda la documentación necesaria para ejercer sus labores dentro de la C.A. VTV, en el momento que se firme el contrato laboral.

Para los trabajadores fijos:

4.2. La información procesada, manipulada o almacenada por el trabajador es propiedad exclusiva de la C.A. VTV.

4.3. La C.A. VTV no se hace responsable por daños causados por sus trabajadores a la información o activos, propiedad de este canal y los efectuados desde sus instalaciones de red a equipos informáticos externos.

a) Capacitación de Usuarios:

4.4. Los usuarios de la red institucional, serán capacitados en cuestiones de seguridad de la información, en función de las actividades que ejecute la Unidad.

4.5. Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación a personal externo o propio de la empresa, siempre y cuando se vea implicada la utilización de los servicios de red o se exponga material de importancia considerable para la empresa.

b) Respuestas a Incidentes y anomalías de seguridad:

4.6. Realizar respaldos de la información, diariamente, para los activos de mayor importancia o críticos, un respaldo semanal que se utiliza en caso de fallas y un tercer respaldo efectuado semestralmente, el cual debe ser guardado y evitar su utilización a menos que sea estrictamente necesaria.

4.7. Se deben eliminar solo respaldos obsoletos y cuentas muy antiguas como parte del mantenimiento para optimizar los servidores solo con autorización de la Gerencia Tecnología de la Información y Comunicación.

4.8. Las solicitudes de asistencia, efectuadas por dos o más trabajadores o unidades de proceso, con problemas en las estaciones de trabajo se otorga solución en el menor tiempo posible.

4.9. Cualquier situación anómala y contraria a la seguridad, debe ser documentada posterior a la revisión de los registros o log de sistemas, con el objeto de verificar la situación y dar una respuesta congruente y acorde al problema en el ámbito legal o cualquier situación administrativa.

Nivel 2: Seguridad Lógica.

1. Control de accesos:

1.1. El Gerente Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe proporcionar toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, guías, controles, otros, localizados en el sistema de gestión de la calidad de la Empresa.

1.2. Cualquier petición de información, servicio o acción proveniente de un determinado usuario se debe efectuar siguiendo los canales de gestión formalmente establecidos por la C.A. VTV para abordar dicha acción; no dar seguimiento a esta política implica:

- Negar por completo la ejecución de la acción o servicio.
- El supervisor inmediato, adscrito a las unidades solicitantes, debe elaborar un informe, dirigido a la Gerencia Tecnología de la Información y Comunicación, y a la Unidad de Auditoría Interna, describiendo la situación presentada.

- Sanciones aplicables por autoridades de nivel superior, previamente discutidas con el Comité de Seguridad.

a) Administración de acceso a los usuarios:

Del ingreso, egreso y ausencia de personal:

1.3. Todos los accesos que proporciona la C.A. Venezolana de Televisión a su personal, deben ser otorgados única y exclusivamente previa existencia de un documento que acredite su relación laboral con la Empresa.

1.4. Es responsabilidad de la Gerencia de Gestión Humana, informar los ingresos y egresos de personal a la Gerencia Tecnología de la Información y Comunicación a través de memorando o mediante el correo electrónico gtic@vtv.gob.ve, con la finalidad de que se tomen las previsiones respectivas en cuanto a los controles de acceso.

1.5. Es responsabilidad del titular de unidad, informar a la Gerencia Tecnología de la Información y Comunicación de los trabajadores que se encuentren ausentes, con la finalidad que se tomen las previsiones respectivas en cuanto a los controles de acceso a los sistemas de información que estén autorizados.

1.6. Son usuarios de la red institucional los trabajadores de la C.A. VTV (planta, administrativos, contratistas y toda aquella persona que tenga contacto directo y utilice los servicios de la red institucional).

1.7. Se debe asignar una cuenta de acceso a los sistemas de la intranet a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que accede, junto a la información personal del usuario.

1.8. Los usuarios externos tienen acceso únicamente a los servicios de internet y recursos compartidos de la red institucional, cualquier cambio sobre los servicios a los que tengan acceso, será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.

1.9. Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con la C.A. VTV fuera del ámbito de trabajador/contratista y siempre que tenga una vinculación con los servicios de la red institucional.

1.10. El acceso a la red por parte de terceros es estrictamente restrictivo, permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad de la C.A. VTV.

1.11. No debe prestarse el servicio solicitado por un usuario o unidad de trabajo, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución según lo establecido en los manuales de normas y procedimientos.

1.12. Se crea una cuenta temporal del usuario una vez se verifiquen y confirmen sus datos de identidad, en caso de olvido o extravío de información de la cuenta institucional, esta debe ser modificada de acuerdo a las pautas establecidas por la Gerencia Tecnología de la Información y Comunicación.

1.13. La longitud mínima de caracteres permisibles en una contraseña se establece en ocho (8) caracteres, los cuales tienen una combinación alfanumérica.

1.14. La longitud máxima de caracteres permisibles en una contraseña se establece en quince (15) caracteres, siendo esta una combinación de mayúsculas y minúsculas.

b) Responsabilidades del usuario:

1.15. El usuario es responsable exclusivo de mantener a excepto su contraseña, uso de su cuenta de acceso a los sistemas o servicios, de incurrir en delitos informáticos conlleva a una denuncia penal por mal uso de los servicios informáticos de la empresa.

1.16. Evitar escribir la contraseña en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guarde en un lugar seguro.

1.17. El usuario es responsable de eliminar de la red cualquier indicio de documentos proporcionados por el Gerente Tecnología de la Información y Comunicación, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

1.18. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionada con su vida o parientes, como fechas de cumpleaños o alguna otra fecha importante.

1.19. El usuario debe proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo

temporal (protector de pantalla) y protegida por una contraseña, esta debe activarse en el preciso momento en que el usuario deje de utilizar el equipo.

1.20. Cualquier usuario que encuentre debilidades de seguridad en los sistemas informáticos autorizados para su uso, está obligado a reportarlo a los administradores del mismo.

1.21. Uso de correo electrónico:

- El servicio de correo electrónico, es un servicio gratuito y uso obligatorio para las comunicaciones institucionales, se debe usar acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red de la empresa.
- El correo electrónico es de uso exclusivo para los trabajadores.
- Todo uso indebido del servicio de correo electrónico, es motivo de suspensión temporal de su cuenta o eliminación total según la falta en que se haya incurrido.
- El usuario es responsable de la información que sea enviada con su cuenta.
- El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores de la red institucional, se reserva el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la empresa.
- El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

c) Seguridad en acceso de terceros:

1.22. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual debe estar firmado por las entidades involucradas en el mismo.

1.23. Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, así como acatar las normas y políticas que devengan de la utilización del mismo.

d) Control de acceso a la red:

Gerencia Tecnología de la Información y Comunicación

1.24. El acceso a la red interna se permite siempre y cuando se cumpla con los requisitos de seguridad requeridos y autorizados mediante un mecanismo de autenticación.

1.25. Eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo afectado en el proceso.

1.26. Cualquier alteración del tráfico de información o datos entrantes o salientes a través de los dispositivos de acceso a la red, será objeto de verificación y tiene como resultado directo la realización de una Auditoría de seguridad.

1.27. Emplear dispositivos de red para el bloqueo, enrutamiento o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

1.28. Los accesos a la red interna o local (Intranet) desde una red externa de la C.A. VTV o extranet, se realizan mediante un mecanismo de autenticación seguro y el tráfico entre ambas redes o sistemas es cifrado bajo un sistema con los últimos protocolos de encriptación.

1.29. Registrar todo acceso a los dispositivos de red, mediante archivos de registro o Log de los dispositivos que provean estos accesos.

1.30. Efectuar una revisión de Log de los dispositivos de acceso a la red en un tiempo máximo de cuarenta y ocho (48) horas.

e) Control de acceso al sistema operativo:

1.31. Deshabilitar las cuentas creadas por ciertas aplicaciones con privilegios de sistema, (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, entre otros) evitando que estas corran sus servicios con privilegios nocivos para la seguridad del sistema.

1.32. Al terminar una sesión de trabajo en las estaciones, los operadores o cualquier otro usuario, debe evitar dejar encendido el equipo, pudiendo proporcionar un entorno de utilización de la estación de trabajo.

Servidores:

1.33. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido por el Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores.

1.34. Los administradores de servicios, tienen acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

1.35. Todo servicio instalado en los servidores, es ejecutado bajo cuentas restrictivas en ningún momento debe obviarse situaciones de servicios corriendo con cuentas administrativas, estos privilegios debe ser eliminados o configurados correctamente.

f) Control de acceso a las aplicaciones:

1.36. Las aplicaciones deben estar correctamente diseñadas, con funciones de acceso específicas para cada usuario del entorno operativo de la aplicación, las prestaciones de la aplicación.

1.37. Definir y estructurar el nivel de permisos sobre las aplicaciones de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o eliminación de información.

1.38. Efectuar revisiones o pruebas minuciosas sobre las aplicaciones informáticas de forma aleatoria sobre sus distintas fases, antes de su instalación en un entorno operativo real a objeto de evitar redundancias en las salidas de información u otras anomalías.

1.39. Las salidas de información de las aplicaciones en un entorno de red, deben ser documentadas y especificar el equipo por donde debe ejecutarse exclusivamente la salida de información.

1.40. Llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, equipos desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

1.41. Registrar y archivar toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

1.42. Los archivos de Log, almacenan nombres de usuarios, nivel de privilegios, IP de equipo, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tenía acceso, entre otros.

1.43. Efectuar una copia automática de los archivos de Log y se envía hacia otro equipo o servidor, evitando que se guarde la copia localmente donde se produce.

2. Gestión de Operaciones y Comunicaciones:

a) Responsabilidades y procedimientos operativos:

2.1. El personal de la Gerencia Tecnología de Información y Comunicación de algún servicio, es responsable absoluto por el óptimo funcionamiento del mismo, coordinar esfuerzos con el coordinador de sistemas con el objetivo de fomentar una cultura de administración segura y servicios óptimos.

2.2. Las configuraciones y puesta en marcha de servicios, deben ser normadas por la Gerencia Tecnología de la Información y Comunicación.

2.3. El personal responsable de los servicios, controla los archivos de los registros por debilidades de seguridad del sistema, revisa estos archivos de forma frecuente y en especial después de ocurrida una falla.

b) Planificación y aceptación de sistemas:

2.4. La Gerencia Tecnología de la Información y Comunicación junto a su personal responsable de la programación o desarrollo de sistemas, efectúa los procesos propios de planificación, desarrollo, adquisición, comparación y adaptación del software necesario para la C.A. VTV.

2.5. La aceptación del software se hace efectiva por la C.A. VTV, previo análisis y pruebas efectuadas por el personal de la Gerencia Tecnología de la Información y Comunicación.

2.6. Únicamente se utiliza software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el unidad de seguridad.

2.7. La aceptación y uso de los sistemas no exonera de responsabilidad alguna sobre el gestor de seguridad, para efectuar pruebas o diagnósticos a la seguridad de los mismos.

2.8. El software diseñado localmente, debe ser analizado y aprobado por el gestor de seguridad, antes de su implementación.

2.9. Es tarea de los programadores el realizar pruebas de validación de entradas, en cuanto a:

- Valores fuera de rango.
- Caracteres inválidos, en los campos de datos.
- Datos incompletos.
- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.
- Procedimientos operativos de validación de errores.
- Procedimientos operativos para validación de caracteres.
- Procedimientos operativos para validación de la integridad de los datos.

2.10. Toda prueba de las aplicaciones o sistemas se debe hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

2.11. Cualquier prueba sobre los sistemas, debe ser documentada y cualquier documento o archivo que haya sido necesario para su ejecución debe ser borrado de los dispositivos físicos, mediante tratamiento electrónico.

c) Protección contra software malicioso:

2.12. Adquirir y utilizar software únicamente de fuentes confiables.

2.13. En caso de ser necesaria la adquisición de software de fuentes no confiables, se debe adquirir en código fuente.

2.14. Los servidores al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente el software antivirus actualizable, así como su activación y protección en tiempo real.

d) Mantenimiento:

2.15. El mantenimiento de las aplicaciones y software de sistemas es responsabilidad exclusiva del personal de la Gerencia Tecnología de la Información y Comunicación.

2.16. El cambio de archivos de sistema, no es permitido sin una justificación aceptable y verificable por el gestor de seguridad.

2.17. Elaborar un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

e) Manejo y seguridad de los medios de almacenamiento:

2.18. Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la C.A. VTV, deben etiquetarse de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

2.19. Los medios de almacenamiento con información crítica o copias de respaldo deben ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el de su salvaguarda.

2.20. Llevar un control, en el que se especifiquen los medios de almacenamiento que debe guardar información y su uso.

Nivel 3: Seguridad Física.

1. Seguridad Física y Ambiental.

a) Seguridad de los equipos:

1.1. El cableado de red, se instala físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica para evitar interferencias.

1.2. Los servidores con problemas de hardware sin importar al dominio o grupo de trabajo al cual estos pertenezcan, deben ser reparados localmente y retirados sus medios de almacenamiento.

1.3. Los equipos o activos críticos de información y proceso, deben ubicarse en unidades aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el Gerente de Tecnología de la Información y Comunicación y las personas responsables de estos activos, quienes debe poseer su debida identificación.

b) Controles generales:

1.4. Las estaciones o equipos de trabajo con procesamientos críticos, no deben contar con medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información.

1.5. En ningún momento se debe dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en que se encuentre de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

1.6. Llevar un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se haga a los equipos.

1.7. Toda unidad de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.

1.8. Toda visita a las unidades de tratamiento de datos críticos e información (unidad de informática, sala de servidores entre otros) debe ser registrada.

1.9. La sala o cuarto de servidores, debe estar separada de las unidades administrativas, Gerencia Tecnología de la Información y Comunicación o cualquier otra unidad o sala de recepción del personal, mediante una división, recubierta de material aislante o protegido contra el fuego. Esta sala debe ser utilizada únicamente por las estaciones prestadoras de servicios y dispositivos a fines.

1.10. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo o en su defecto, el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

1.11. El suministro de energía eléctrica debe tener una red de polarización, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente.

1.12. Las instalaciones de las unidades de trabajo, deben contar con una adecuada instalación eléctrica y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para proteger la información.

1.13. Las salas o instalaciones físicas de procesamiento de información, debe poseer información en carteles para su acceso, alimentos o cualquier otra actividad contraria a su seguridad o información que procesa.

Nivel 4: Seguridad Legal.

2. Conformidad con la Legislación.

a) Cumplimiento de requisitos legales:

Licenciamiento de software:

2.1. La C.A. Venezolana de Televisión se reserva el derecho de respaldo a cualquier miembro usuario de la red o miembro de las unidades administrativas, ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.

2.2. Todo el software comercial que utilice la C.A. Venezolana de Televisión, debe estar legalmente registrado en los contratos de arrendamiento de software con sus respectivas licencias.

2.3. La adquisición de software por parte del personal que labora en la C.A. VTV, no expresa el consentimiento de esta Empresa, la instalación del mismo no garantiza responsabilidad alguna para la misma, por ende la C.A. VTV no se hace responsable de las actividades de sus trabajadores.

2.4. Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores, la C.A. VTV respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores y las responsabilidades inherentes al licenciamiento de software libre son responsabilidad absoluta de la C.A. VTV.

2.5. El software comercial licenciado para la C.A. VTV, es propiedad exclusiva de la empresa la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores respetando el esquema de cero piratería y distribución a terceros.

2.6. En caso de transferencia de software comercial a terceros, se realizan las gestiones necesarias para su efecto y se acatan las medidas de licenciamiento relacionadas con la propiedad intelectual.

2.7. El software desarrollado internamente por el personal que labora en la C.A. VTV es propiedad exclusiva de la misma.

2.8. Cualquier cambio en la política de utilización de software comercial o software libre, se realiza documentado y en base a las disposiciones de la respectiva licencia.

2.9. La adquisición del software libre o comercial, debe ser gestionado con las autoridades competentes y acatando sus disposiciones legales, en ningún momento se obtiene software de forma fraudulenta.

2.10. Los contratos con terceros para la gestión o prestación de un servicio, deben especificar las medidas necesarias de seguridad, nivel de prestación del servicio y el personal involucrado en el proceso.

b) Revisión de políticas de seguridad y cumplimiento técnico:

2.11. Toda violación a las políticas de licenciamiento de software, es motivo de sanciones aplicables al personal que incurra en mismo.

2.12. El documento de seguridad debe ser elaborado y actualizado por la División de Planificación, adscrita a la Gerencia de Planificación y Presupuesto, su aprobación y puesta en ejecución es responsabilidad de todas las unidades organizativas de la C.A. VTV.

2.13. Cualquier violación a la seguridad por parte del personal que labora en la C.A. VTV, así como terceros que tengan relación o alguna especie de contrato con esta Empresa se hacen acreedores a sanciones aplicables de ley.

c) Consideraciones sobre auditorías de sistemas:

2.14. Se debe efectuar una auditoría de seguridad a los sistemas de acceso a la red de forma semestral, enmarcada en pruebas de acceso tanto internas como externas, desarrolladas por personal técnico especializado o en su defecto personal capacitado en la Gerencia Tecnología de la Información y Comunicación.

2.15. Cualquier acción que amerite la ejecución de una auditoría a los sistemas informáticos, debe ser documentada, establecer su aplicabilidad, objetivos, personal involucrado y sistemas implicados.

2.16. La auditoría no debe modificar en ningún momento el sistema de archivos implicados, en caso de haber necesidad de cambios, se debe hacer un respaldo formal del mismo.

2.17. Las herramientas utilizadas para la auditoría, deben estar separadas de los sistemas de producción y no al alcance del personal responsable de su elaboración.

Normas de Seguridad Informática

Nivel 1: Seguridad Organizacional

1. En cuanto a Políticas Generales de Seguridad

   Gerencia Tecnología de la Información y Comunicación:

   1.1. El usuario debe acatar las disposiciones expresas sobre la utilización de los servicios informáticos de la red institucional.

   1.2. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, realiza respaldos periódicos de la información así como la depuración de los discos duros.

   1.3. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe realizar auditorías periódicas en el sistema con el fin de localizar intrusos o usuarios que estén haciendo mal uso de los recursos de un servidor.

   1.4. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe tomar decisiones sobre el uso de los recursos del sistema, restricción de directorios y programas ejecutables para los usuarios.

   1.5. Revisar el tráfico de paquetes que se estén generando dentro de un segmento de red, a fin de determinar si se está haciendo mal uso de la red o se está generando algún problema que pueda llevar a que se colapsen los sistemas.

   1.6. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, deben:

   - Crear, eliminar a los usuarios y revisar las cuentas periódicamente para estar seguros de que no hay usuarios ficticios.
   - Recomendar sobre el uso e implementación de nuevas tecnologías para administración de los sistemas y la red.
   - Reportar a la Presidencia o Vicepresidencia Ejecutiva, las debilidades en el desempeño de la red.
   - Solucionar los problemas que se generen en su red local.

   1.7. La C.A. VTV se reserva el derecho de divulgación o confidencialidad de la información personal de los usuarios de la red institucional, si estos se ven envueltos en actos ilícitos.

1.8. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, deben:

- Monitorear las acciones y tareas de los usuarios de la red institucional.
- Prestar servicio de Internet, siempre que se encuentren presentes los requisitos de seguridad mínimo y considerable establecido en la Políticas de Seguridad de Datos e Información.
- Suspender cualquier usuario que utilice los equipos fuera del ámbito institucional y los objetivos para los que estos fueron creados.

2. Excepciones de Responsabilidad:

2.1. La C.A. VTV, debe establecer con sus trabajadores un contrato de confidencialidad.

2.2. Toda acción debe seguir los canales de gestión necesarios para su ejecución.

2.3. El nivel ejecutivo, debe proveer la documentación necesaria para aprobar un acuerdo de no responsabilidad por acciones que realicen dentro de la red institucional.

2.4. Las gestiones para las excepciones de responsabilidad son acordadas bajo común acuerdo de la Gerencia Tecnología de la Información y Comunicación y el Comité de Seguridad.

3. Clasificación y Control de Activos

a) Responsabilidad por los activos:

3.1. El titular de cada unidad, es responsable de los activos asignados a la misma.

3.2. Los responsables de cada unidad organizativa de la C.A. VTV, deben mantener o proteger los activos de mayor importancia.

b) Clasificación de la información:

3.3. Cada responsable proporciona importancia a la información, en base al nivel de clasificación que demande el activo.

3.4. La información pública puede ser visualizada por cualquier persona dentro o fuera de la C.A. VTV

3.5. La información interna es propiedad del contratista y de la C.A. VTV, en ningún momento intervienen personas ajenas a su proceso o manipulación. La información confidencial es propiedad absoluta de la C.A. VTV, el acceso a ésta es permitido únicamente a personal debidamente autorizados por las autoridades competentes.

3.6. Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.

4. Seguridad Ligada al Personal

Referente a contratos:

4.1. Todo trabajador ejerce las labores estipuladas en su contrato de trabajo.

El trabajador.

4.2. El trabajador no tiene ningún derecho, sobre la información que sea procesada dentro de las instalaciones de la red institucional.

4.3. La información que maneja o manipula el trabajador, no puede ser divulgada a terceros o fuera del ámbito de laboral.

4.4. El usuario se rige por las disposiciones de seguridad informática de la C.A. VTV.

4.5. El usuario es responsable de las acciones causadas por operaciones con el equipo y la red institucional.

a) Capacitación de usuarios:

4.6. La Gerencia Tecnología de la Información y Comunicación, es responsable de capacitar a los usuarios de la red institucional, por unidad organizativa y en el sitio destinado para tal fin.

4.7. La Gerencia de Gestión Humana, establece las fechas en que se realicen las capacitaciones.

4.8. El material de apoyo (manuales, guías, entre otros), debe ser entregado minutos antes de iniciar la capacitación.

4.9. En cada capacitación se deben revisar con anticipación, los dispositivos de conexión de servicios involucrados en la capacitación.

4.10. Entre los deberes y derechos de los trabajadores fijos y personal contratado, deben acatar o respetar las disposiciones sobre capacitación y por ende asistir a ellas sin excepción, Excepto casos especiales.

b) Respuesta a incidentes y anomalías de seguridad:

4.11. Los respaldos de información deben ser almacenados en un sitio aislado y libre de cualquier daño o posible extracción por terceros dentro de la C.A. VTV.

4.12. La C.A. VTV, debe contar con respaldos de la información ante cualquier incidente.

4.13. Generar manuales de nomas y procedimientos para el respaldo de la información junto con la División de Planificación.

4.14. La Gerencia Tecnología de la Información y Comunicación, tiene la responsabilidad de priorizar casos en cuanto a los problemas en las estaciones de trabajo.

4.15. En situaciones de emergencia que impliquen unidades de atención al cliente entre otros, se establece prioridad en el siguiente orden:

- Gerencia de Planificación y Presupuesto.
- Gerencia de Administración y Finanzas
- Consultoría Jurídica.

4.16. El documento de seguridad, debe elaborarse tomando en cuenta aspectos basados en situaciones pasadas y enmarcarlo en la pro actividad de situaciones futuras.

4.17. Priorizar la información de mayor importancia para la C.A. VTV.

4.18. Evaluar la información o activo de los niveles confidenciales de la C.A. VTV.

4.19. Respaldar los archivos logs o registro de los sistemas en proceso, cada cierto tiempo durante el día.

4.20. Llevar un registro de las actividades sospechosas de los trabajadores.

Nivel 2: Seguridad Lógica

1. Control del Acceso de Usuarios a la Red Institucional:

1.1. Toda documentación relacionada con formularios, guías, entre otros, debe ser elaborada por la unidad responsable a través el sistema vigente.

1.2. La documentación de seguridad debe ser resguardada por el Gerente de Tecnología de la Información y Comunicación, esto incluye folletos, guías, formularios, controles entre otros.

1.3. Los canales de gestión y seguimiento para realizar acciones dentro de la red institucional, no pueden ser violentados bajo ninguna circunstancia.

1.4. El personal encargado de dar soporte a la gestión de comunicaciones, no está autorizado a brindar ninguna clase de servicios, mientras no se rija por los procedimientos establecidos en la C.A. VTV.

a) Administración del acceso de usuarios a los servicios informáticos de la C.A Venezolana de Televisión:

1.5. Sin excepción alguna se consideran usuarios de la red institucional de la C.A. Venezolana de Televisión todos y cada uno del personal que se encuentra descrito en este documento.

1.6. El acceso a los sistemas y servicios de información, es permitido únicamente a los usuarios que dispongan de los permisos necesarios para su ejecución. El usuario debe proveer toda la información necesaria para poder brindarle los permisos necesarios para la ejecución de los servicios de la red institucional.

1.7. Las necesidades y aprobación de acceso de los usuarios a los servicios de la red institucional, debe ser documentada, así como actualizar su información, en la política que orienta su uso.

1.8. La vinculación de servicios por parte de terceros con la red institucional, es característica propia del personal en outsourcing, contratistas, proveedores de software.

1.9. Cualquier petición de servicio por parte de personal de la C.A. VTV o ajeno a la misma, no se concede sino es mediante la aprobación de la política de acceso y prestación de servicio.

1.10. La cuenta temporal es usada únicamente con propósitos legales y de ejecución de tareas por olvido de la información de la cuenta personal. La cuenta temporal es únicamente acreditable, si se proporciona la información necesaria para su uso.

1.11. Toda cuenta nula u olvidada se eliminara del (los) sistema(s), previa verificación o asignación de una nueva cuenta al usuario propietario de la misma.

1.12. El usuario/contraseña temporal, será eliminada del sistema por el personal de la Gerencia Tecnología de la Información y Comunicación en el momento en que sea habilitada una cuenta personal para el usuario que haya solicitado su uso.

1.13. El sistema no acepta contraseñas con una longitud menor a la expresada en la política de creación de contraseñas.

1.14. Los usuarios deben realizar un seguimiento estricto sobre las políticas de creación de contraseñas, acatando sus disposiciones en su totalidad.

1.15. El sistema revoca toda contraseña con una longitud mayor a la expresada en la política de creación de contraseñas.

1.16. El usuario se responsabiliza en crear una contraseña fuerte y segura.

b) Responsabilidades del usuario:

1.17. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe desactivar cualquier característica de los sistemas o aplicaciones que permita a los usuarios, almacenar localmente las contraseñas.

1.18. El usuario, debe estar consciente de los problemas de seguridad que acarrea la irresponsabilidad en salvaguardar el uso de la contraseña.

1.19. El usuario, debe ser precavido al manipular la cuenta de acceso a los sistemas, tomando medidas de seguridad que no pongan en riesgo su integridad como persona.

1.20. Las cuentas de usuario son personales, en ningún caso deben ser utilizadas por personal ajeno al que le fue asignada.

1.21. La práctica de guardar las contraseñas en papel adherido al monitor o unidades cercanas al equipo de trabajo, es una falta grave y sancionable.

1.22. Las contraseñas deben ser memorizadas o archivadas bajo su responsabilidad.

1.23. Desechar, toda documentación que tenga que ver con información relacionada a su cuenta de usuario, minutos después de habérsele entregado y siempre que haya sido memorizada o resguardado bajo su responsabilidad.

1.24. Es importante que el usuario establezca contraseñas fuertes y desligadas de su vida personal o de su entorno familiar, no emplear formatos comunes de fechas.

1.25. El servidor de dominio, debe bloquear cualquier estación de trabajo con un protector de pantalla, que tenga un tiempo de inactividad mayor a un minuto.

1.26. El usuario es parte esencial en la seguridad de la información y debe reportar a la Gerencia Tecnología de la Información y Comunicación, a través del operador de las estaciones de trabajo cualquier anomalía presentada en su equipo.

Uso de correo electrónico:

1.27. El correo electrónico es un medio de comunicación directo y confidencial, entre el emisor del mensaje y el receptor o receptores del mismo, por ende debe ser visto o reproducido por las personas que intervienen en la comunicación.

1.28. Ningún usuario externo a la C.A. VTV, puede usar los servicios de correo electrónico proporcionado por la red institucional.

1.29. Es responsabilidad del usuario hacer un correcto empleo del servicio de correo electrónico.

1.30. Cualquier actividad no consecuente con los ítems que se describen a continuación se consideran como uso indebido del correo electrónico:

- Abuso de comunicaciones con fines personales.
- Comunicaciones con clientes para concertar negocios propios, ajenos a la empresa.
- Fuga de información confidencial de la empresa.
- Hurto de "intangibles" de la empresa (por ejemplo, software).
- Tráfico de material pornográfico.
- Comisión de acciones tipificadas como ilícitas (como, por ejemplo, injurias y hurto de información, entre otras).
- Tráfico ilegal de obras protegidas (software, imágenes y música).
- El fraude, la deslealtad y el abuso de confianza en las gestiones encomendadas.
- La desobediencia a las órdenes de los superiores, así como el incumplimiento de las normas específicas de la entidad que impliquen quebranto manifiesto de disciplina o de ellas derive grave perjuicio para la empresa.
- La utilización fraudulenta de los medios electrónicos o herramientas tecnológicas establecidas en la empresa.
- La reincidencia en la comisión de faltas graves, aunque sean de distinta naturaleza.

Además en la normativa interna de la empresa se prohíbe:

1.31. Reenviar mensajes y documentos de la empresa a cuentas privadas del trabajador o de sus familiares o amigos, debido a que no gozan del mismo nivel de seguridad.

1.32. Tampoco se puede configurar la cuenta de correo institucional para reenviar los mensajes recibidos a una cuenta de correo electrónico privado.

c) Seguridad en acceso de terceros:

1.33. Al ser contratado para cumplir funciones en el ámbito de su competencia dentro de las instalaciones de la C.A. VTV, se realiza entrega de la documentación necesaria para cubrir todas las necesidades inherentes a su cargo.

1.34. Los requisitos mínimos de seguridad se expresan, en cuestión del monitoreo y adecuación de un servicio con respecto a su entorno o medio de operación. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores debe tomar las medidas necesarias para asignar los servicios a los usuarios externos.

1.35. El no cumplimiento de las disposiciones de seguridad y responsabilidad sobre sus acciones por parte de los usuarios de la red institucional, se obliga a la suspensión de su cuenta de usuario de los servicios.

d) Control de acceso a la red:

1.36. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, es responsable de diseñar los mecanismos necesarios para proveer acceso a los servicios de la red institucional.

1.37. Los mecanismos de autenticación y permisos de acceso a la red, debe ser evaluados y aprobados por el Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores.

1.38. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, realiza evaluaciones periódicas a los sistemas de red, con el objetivo de eliminar cuentas de acceso sin protección de seguridad, componentes de red comprometidos.

1.39. El personal que presta soporte de escritorio remoto debe efectuar la conexión desde un equipo personal, en ningún momento lo debe realizar desde una red o unidad de servicios públicos.

1.40. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe verificar:

- Que los recursos del sistema permitan medir la recepción o transmisión de información, la cantidad de usuarios y tráfico de red.
- Que los dispositivos de red, estén activos y configurados correctamente para evitar anomalías en el tráfico y seguridad de información de la red institucional.
- Que se utilicen mecanismos y protocolos de autenticación como, ssh, Ipsec, claves públicas y privadas, autenticación usuario/contraseña, cualquiera de ellos será válido para la misma.
- Que los archivos de registro o logs de los dispositivos de red, estén activados y configurados correctamente, en cada dispositivo.

e) Monitoreo del acceso y uso del sistema

Personal de tecnología:

1.41. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe tener cuidado al momento de instalar aplicaciones en los servidores, configurando correctamente cada servicio con su respectivo permiso de ejecución.

1.42. La finalización de la jornada laboral, termina con cualquier actividad desarrolla en ese momento, lo cual implica guardar todo cuanto se utilice y apagar equipos informáticos antes de salir de las instalaciones.

1.43. El servidor de dominios, verifica y desactiva cualquier estación de trabajo, que este en uso después de la hora de salida o finalización de la jornada laboral.

1.44. No está permitido al usuario, realizar actividades de configuración del sistema, bajo ninguna circunstancia.

1.45. Los servidores están debidamente configurados, evitando el abuso de personal extraño a su administración.

1.46. En el caso de tener la necesidad de efectuar configuración de servicios por más de un usuario el Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe permitir acceso exclusivo mediante una cuenta referida al servicio.

1.47. La cuenta administrativa es monitoreada por el Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores.

1.48. Las aplicaciones prestadoras de servicios corren con cuentas restrictivas y jamás con privilegios tan altos como los de la cuenta administrativa.

f) Control de acceso a las aplicaciones:

1.49. Las aplicaciones deben contar con su respectiva documentación, la cual se entrega a cada trabajador de la C.A. VTV.

1.50. El usuario tiene los permisos de aplicaciones que requiera dentro del ámbito de competencia previa autorización del titular de la unidad donde presta sus funciones.

1.51. Los niveles de privilegio son definidos por el Comité de Seguridad en base a lo importante o crítico de la información que deba procesar el usuario.

1.52. Toda aplicación ante de ser puesta en ejecución, debe realizarse una Auditoría sobre fallos o información errónea que puedan procesar.

1.53. Se hace énfasis en la importancia que tienen las salidas de información provistas por una aplicación, sin importar el medio de salida.

1.54. El Técnico apoyado por el Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, deberá:

- Depurar el código de las aplicaciones, antes de ser puestas en marcha.
- Llevar un seguimiento en limpio sobre que equipos es posible efectuar las salidas de información desde el servidor.
- Registrar en el sistema vigente para tal fin, los sucesos y actividades realizadas por un determinado usuario, sobre las aplicaciones.
- Visualizar información, únicamente en equipos previamente definidos, mediante direccionamiento de hardware o direccionamiento IP.
- Verificar constantemente la operatividad de los registros de logs, que no sean alterados de forma fraudulenta.

g) Respuesta a incidentes y anomalías de seguridad:

1.55. Los archivos de registro de sucesos de los sistemas de aplicación y de operación, se mantienen siempre activos y en ningún momento debe ser deshabilitados.

1.56. De ser necesario, debe crearse archivos para la ejecución de comandos por lotes para verificar que se cumpla el grabado completo de la información a la que es accedida por los usuarios, aplicaciones, sistemas y para los dispositivos que guardan estos archivos.

1.57. Los archivos de registro o logs, deben ser respaldados en tiempo real y los nombres muestran la hora y la fecha en la que fueron creados en original.

2. Gestión de Operaciones y Comunicaciones

a) Responsabilidades del usuario sobre los procedimientos operativos:

2.1. La Gerencia Tecnología de la Información y Comunicación, es quien crea las reglas para la ejecución de algún servicio.

2.2. Los sistemas son configurados para responder de forma automática, con la presentación de un informe que denote las características propias de un error en el sistema.

b) Planificación y aceptación de sistemas:

2.3. Ninguna otra persona que no sea la expresada en la política de aceptación y creación de sistemas puede intervenir, sino es por petición expresa de alguna de estas.

2.4. Ninguna persona que labore para la Empresa, está facultada para instalar software en las estaciones de trabajo, sin antes haberse aprobado su utilización.

2.5. Sin importar el origen del software y la utilización del mismo dentro de la C.A VTV, éste debe ser evaluado, con aprobación o no de su utilización.

2.6. Ninguna clase de código ejecutable será puesto en marcha sin antes haber pasado el control de análisis sobre seguridad del mismo.

2.7. Antes de efectuar cualquier análisis o prueba sobre los sistemas de producción, se realizan respaldos o backups generales de la información que en ellos se procesa y del sistema en sí.

2.8. Los sistemas o dispositivos que aún están conectados a la red, pero que no tienen utilización productiva alguna para la C.A. VTV, deben eliminarse.

c) Protección contra software malicioso:

2.9. El software que se reciba de empresas no reconocidas o acreditadas como no confiables, no tiene valor alguno para la C.A. VTV siempre que esta sea en formato ejecutable.

2.10. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, supervisa la instalación y la correcta configuración de software antivirus en todas las estaciones de trabajo de la C.A VTV.

d) Mantenimiento de sistemas y equipo de cómputo:

2.11. El usuario no está facultado a intervenir física o lógicamente ninguna estación de trabajo, que amerite reparación.

2.12. En ningún momento es aceptable la modificación de archivos en los equipos informáticos, sino es bajo circunstancias especiales, en las que de no hacerse de esa manera el sistema queda inutilizable.

2.13. En caso de ser afirmativo el cambio de archivos se realiza un respaldo o backup general de la aplicación o sistema al cual se le realiza el cambio.

2.14. Cualquier falla efectuada en las aplicaciones o sistemas por la manipulación errónea de archivos, posterior mantenimiento debe ser notificada y reparada por el personal técnico encargado en dicha función.

2.15. Se debe hacer una bitácora completa, en cuando a las versiones de actualización del software y de las revisiones instaladas en los sistemas.

e) Seguridad en el manejo de los medios de almacenamiento:

2.16. La clasificación e identificación de los medios de almacenamiento, es acorde al propósito u objetivo por el cual se respalda.

2.17. Bajo ninguna circunstancia debe ser desatendidos los medios de almacenamiento, o copias de seguridad de los sistemas.

2.18. Todo medio de almacenamiento debe ser documentado e inventariado, en un registro específico y único sobre medios de almacenamiento.

2.19. La ubicación de los medios de almacenamiento deben estar alejado del polvo, humedad, o cualquier contacto con material o químicos corrosibles.

2.20. La llave de seguridad que permite el acceso a los medios de almacenamiento resguardados bajo supervisión de la Gerencia, será mantenida bajo estricta seguridad por cualquiera de las dos entidades encargadas de mantener la seguridad de los medios.

2.21. Entre la documentación de seguridad debe existir un control para la clasificación y resguardo de los medios de almacenamiento.

Nivel 3: Seguridad Física

1. La Seguridad en las Diferentes Unidades de Procesamiento de Información.

a) Resguardo de los equipos de cómputo

Usuarios comunes y administrativos:

1.1. La División de Redes y Servidores, debe diseñar toda la red de la Empresa siguiendo la normativa de cableado estructurado.

1.2. Esta totalmente prohibido, Excepto autorización o supervisión expresa de la División de Redes y Servidores, la intervención física de los usuarios sobre los recursos de la red institucional (cables, enlaces, estaciones de trabajo, dispositivos de red).

1.3. Solo el personal autorizado es el encargado exclusivo de intervenir físicamente los recursos de la red institucional.

Personal de Informática:

1.4. El soporte técnico a las estaciones de trabajo y servidores, es responsabilidad de la División de Redes y Servidores, por tanto deben tomarse todas las medidas de seguridad necesarias para evitar cualquier anomalía por manipulación errónea efectuada por terceros.

1.5. Las estaciones de trabajo y servidores, deben operar en óptimas condiciones, efectuando un mantenimiento constante y acorde a las especificaciones de los fabricantes del equipo.

1.6. Realizar la protección a las salas que contengan los servidores, o equipos de información críticos, con paredes recubiertas de material aislante o anti incendios.

1.7. Las líneas de alimentación de energía externa debe estar protegidas con filtros de protección para rayos.

1.8. Los centros de procesamiento de datos o unidades de procesos críticos, son zonas restringidas, únicamente accesibles por personal autorizado o que labore en dichas instalaciones.

1.9. Al permanecer en las instalaciones de procesamiento de información, se enfoca exclusivamente a los procesos relacionados con las actividades propias del centro de

procesamiento, evitando cualquier actividad contraria a los objetivos para los que fue diseñada.

1.10. El personal debe contar con su respectiva identificación, donde se reconoce su nombre, unidad de trabajo, cargo que desempeña dentro de dicha unidad y su fotografía.

1.11. Cada estación de procesamiento crítico de información debe estar protegido con un dispositivo de alimentación ininterrumpida, que debe ser de uso exclusivo para dicha estación.

b) Controles físicos generales:

1.12. Los respaldos de información de las estaciones de procesos críticos, solo lo realiza el personal responsable de dicho proceso.

1.13. Las disqueteras, unidades USB y lectoras de CD debe deshabilitarse en aquellos equipos en que no se necesiten.

1.14. Cada trabajador de la C.A VTV, debe velar por la correcta salvaguarda de la información, el dejar información desatendida sin ningún medio de seguridad verificable es una práctica prohibida y sancionable.

1.15. Establecer los periodos de mantenimiento preventivo.

1.16. El Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores, debe llevar el registro del mantenimiento que se realizan a los equipos de cómputo.

1.17. No se permite el ingreso a las instalaciones de procesos críticos, sin antes haberse completado el proceso de registro de información, en el documento especificado para ese uso.

1.18. Las instalaciones de la División de Redes y Servidores, debe contar con un espacio dedicado única y exclusivamente a la unidad de servidores, la cual se mantiene separado mediante una división de pared y protegido su acceso bajo llave. Cualquier actividad anómala, efectuada dentro de las instalaciones físicas de procesamiento de información debe ser cancelada en el momento en que se constatase la actividad.

1.19. El personal de la Gerencia Tecnología de la Información y Comunicación es relevado de su cargo, si no está cumpliendo con las actividades asignadas y esté utilizando su tiempo a realizar actividades extrañas a los objetivos de la misma.

1.20. Al ingresar a la Gerencia Tecnología de la Información y Comunicación, se da por aceptada la normativa de permanencia en las instalaciones, desarrollada bajo la política de acceso y permanencia en las unidades. Los equipos de oficina, como cafeteras, aires acondicionados, entre otros no deben estar conectados al mismo circuito que los sistemas informáticos.

1.21. Realizar una revisión periódica de los equipos de respaldo de energía o UPS, constatando su capacidad y correcto funcionamiento, se registra cada revisión en una bitácora de control y funcionamiento de los equipos.

1.22. Es responsabilidad de los usuarios la correcta utilización de los equipos de respaldo de energía o UPS y son de uso exclusivo de cada estación de trabajo.

1.23. Al finalizar con la jornada laboral es necesario que cada usuario de las estaciones de trabajo verifique el apagado correctamente el equipo y dispositivo UPS.

1.24. Se debe efectuar una revisión periódica de los circuitos.

1.25. Es responsabilidad del Gerente de Tecnología de la Información y Comunicación/Jefe de División de Redes y Servidores proveer los materiales informativos (carteles) necesarios en las diferentes salas o instalaciones físicas de procesamiento de información.

1.26. El material debe ser claramente entendible y visible por todos los usuarios.

2. Actividades prohibitivas:

2.1. Está prohibido el ingreso de bebida(s) o alimento(s) de cualquier tipo a las unidades, sin la aprobación de la persona encargada.

2.2. Se prohíbe a los usuarios utilizar equipos informáticos, herramientas o servicios provistos por la C.A. VTV para un objetivo distinto del que están destinadas o para beneficiar a personas ajenas a esta.

2.3. Se prohíbe el ingreso de personas en estado de embriagues sin importar el cargo que desempeñen, a las unidades críticas o no, para la C.A. VTV.

Nivel 4: Seguridad Legal

3. Conformidad con la Legislación

a) Cumplimiento de requisitos legales:

3.1. Las acciones de los trabajadores de la C.A. VTV referente a la utilización de software pirata dentro de sus instalaciones no son propias de la misma.

3.2. La C.A. VTV se reserva todo derecho al utilizar software licenciado en sus equipos de producción, bajo ninguna circunstancia se aprueba la utilización de software sin la licencia requerida.

3.3. La Gerencia Tecnología de la Información y Comunicación, debe realizar un control detallado sobre los inventarios de software referente a sus licencias y contratos firmados para ser utilizados en la infraestructura tecnológica de la red institucional.

3.4. El original de los contratos de arrendamiento de software, debe ser resguardado por la Gerencia Tecnología de la Información y Comunicación.

3.5. La C.A. VTV participa con la Gerencia Tecnología de la Información y Comunicación en la adquisición de software en forma legal.

3.6. Ningún trabajador puede instalar software no licenciado en los equipos de trabajo, los cuales son propiedad exclusiva del propietario intelectual del software.

3.7. La C.A. VTV desecha por completo la utilización de software pirata o no licenciado en las estaciones de trabajo, servidores y equipo informático personalizado, que sea parte de sus inventarios informáticos.

3.8. El contrato de licencia de usuario final tanto de software comercial con derechos de copyright, como de software libre con derechos de copyleft, son respetados en su totalidad por la C.A. VTV, los trabajadores no pueden utilizar software de este tipo sin su respectiva licencia.

3.9. La C.A. VTV a razón de seguridad de sus activos, realiza copias de seguridad de software que son licenciadas en el contrato de arrendamiento, con el objetivo de resguardar la licencia original y su medio físico.

3.10. Las copias que se hagan del software original están destinadas para las instalaciones en toda la red institucional.

3.11. La transferencia de software comercial a terceros, es una actividad únicamente permisible por un derecho concedido a la C.A. VTV por el propietario intelectual del software o licencia en cuestión.

3.12. La C.A. VTV no hace uso indebido de estas licencias, obteniendo provecho por su distribución si no es acordado por su contrato de licencia de derechos de autor.

3.13. El software libre es regido por la licencia GPL y concedido a la C.A. VTV con derechos de copyleft, por tanto, no es permitido en ningún momento la distribución ilegal de este software, haciéndose acreedor la Empresa o trabajadores de los derechos de propiedad intelectual.

3.14. Al laborar para la C.A. VTV, cualquier información, código u otros, producida, mediante tratamiento electrónico dentro de sus instalaciones es propiedad irrevocable de la empresa.

3.15. Ningún trabajador de la C.A. VTV, está facultado a obtener software para su uso dentro de esta Empresa, solo las unidades y autoridades autorizadas que encuentren facultado para tal fin.

b) Cumplimiento técnico de la revisión y actualización de las políticas de seguridad:

3.16. La documentación de seguridad descrita, puede ser actualizada respetando todas y cada una de las políticas que demandan su correcto diseño y aplicabilidad.

3.17. En ningún momento, personal ajeno y responsables de la actualización y aprobación de ésta documentación, debe ser designados como propietarios de los cargos de actualización y aprobación de los mismos, sin antes haber aprobado una preparación técnica para tales efectos.

3.18. El personal o usuarios de la red institucional, debe tener pleno conocimiento de la documentación de seguridad, apegarse a ella en todo caso o gestión.

3.19. El medio exclusivo de soporte para la seguridad en el tratamiento de la información de la C.A. VTV, lo constituyen las políticas de seguridad informática y toda su reglamentación técnica, esto incluye un sistema de gestión de seguridad de la información.

3.20. Se suspende por plazo de hasta un año por incumplimiento de la normativa de seguridad informática o de protección de datos en los casos en que los problemas ocasionados sean críticos y vitales para el correcto funcionamiento de la C.A. VTV

3.21. El único caso en el que personal contratado o fijo no sea sancionado por infracción a la seguridad informática de la empresa, serán los previstos en la política de excepciones de responsabilidad.

c) Normativa Sobre Auditorías a los Sistemas de Información:

3.22. La ejecución de una auditoría a los sistemas informáticos, amerita la planificación de la misma, la herramienta a utilizar, objetivos, implicaciones legales, contractuales, requisitos en conformidad a la Empresa.

3.23. De no existir personal técnicamente preparado para efectuar auditorías a la seguridad de la información, estos deben ser capacitados por personal especializado en la unidad.

3.24. Excepto casos especiales toda auditoría, debe estar respaldada por la Empresa.

3.25. Los casos especiales que ameriten la aplicación de auditorías no requieren de fechas planificadas.

3.26. En toda auditoría se debe llevar un control exhaustivo en cuanto a el registro de la actividad relacionada, quienes la realizan, fechas, horas y todo lo que involucre dicha auditoría.

3.27. El personal de auditoría no está facultado a realizar cambios en los sistemas informáticos, tanto en los archivos que integran el sistema o de la información que en ellos se procesa.

3.28. Excepto caso especial, cualquier cambio efectuado al sistema de archivos, será motivo de sanción.

3.29. Las auditorías a los sistemas, deben ser realizadas con equipos móviles (Laptops) conectados a la red, en ningún momento el sistema de producción mantendrá instalado software para auditoría en su disco duro.

3.30. Toda aplicación informática autorizada para la auditoría, debe ser instalada y supervisada desde los equipos remotos en el mismo segmento de red.