


## COPIA NO CONTROLADA

	SEGURIDAD INFORMATICA	Código: TE-TEI-PO-002
		Tipo: POLITICA
		Vigencia: 2014-09-20
		Versión: 002

## 1. OBJETO

Los objetivos esenciales de esta política son:

Proveer los procedimientos y normas generales para llevar a cabo la Administración de Seguridad Informática que apoyen al personal de Tecnología de la Información, brindándole una guía informativa del proceso y manejo de la Seguridad Informática.

Otorgar la información necesaria detalladamente a los usuarios, empleados y proveedores de la Organización de las normas y mecanismos que deben cumplir y utilizar para la protección de todo lo relacionado a la Infraestructura de Tecnología de la Información

Los servicios a través de la Infraestructura de Tecnología de la Información de TEAM son una herramienta valiosa en el manejo diario de los procesos informáticos de la empresa pero también de un mal uso dado al servicio se pueden llegar a tener una serie de problemas que afectan la seguridad tanto de la red como de los usuarios finales

## 2. ALCANCE

Aplica a todos los funcionarios de las empresas Team Foods y sus filiales, proveedores o contratistas del área de Tecnología de la Información, Auditores y en general a toda persona natural o jurídica que tenga una relación directa o indirecta con el área de Tecnología de la Información de Team Foods, quienes por sus funciones requieren una serie de servicios informáticos para el desempeño diario de su trabajo o de alguna labor en particular lo cual le permite interactuar con los demás usuarios y con el medio global ya que muchas de la formas de negocio de hoy en día se manejan a través de medios electrónicos

## 3. RIESGO(S) ASOCIADO(S)

La mayoría de los desastres se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones, robos, etc. Y aunque no se pueda prevenir cada una de estas interrupciones, la organización sí puede prepararse para evitar las consecuencias que éstas puedan tener sobre su negocio. Del tiempo que tarde en reaccionar una empresa dependerá la gravedad de sus consecuencias

## 4. DEFINICIONES

**4.1 Administración Remota:** Forma de administrar los servidores, computadores o dispositivos informáticos o servicios de la Organización, a través de terminales o equipos remotos, físicamente separados del equipo.

**4.2 Amenaza:** Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

**4.3 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, terminales o IP's involucradas en el proceso, etc.)

**4.4 Ataque:** Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

**4.5 Confidencialidad:** La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

**4.6 Cuenta de Usuario:** Mecanismo de identificación de un usuario, llamado de otra forma es el método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.

- 4.7 Desastre:** Interrupción en el funcionamiento normal de un sistema, con pérdidas materiales y económicas que afectan un trabajo o proceso.
- 4.8 Disponibilidad:** Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- 4.9 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.
- 4.10 Hardware:** Conjunto de los componentes que integran la parte física o material de una computadora.
- 4.11 Impacto:** consecuencia de la materialización de una amenaza
- 4.12 Integridad:** Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- 4.13 Responsabilidad:** En términos de seguridad, significa determinar qué áreas o personas en la organización son responsables directas de mantener seguros los activos de Tecnología de la Información.
- 4.14 Riesgo:** Posibilidad de que se produzca un Impacto determinado en un Activo, que afecte a toda la Organización.
- 4.15 Servicio:** Conjunto de aplicativos o programas que apoyan la labor sobre los procesos diarios que requieran información o comunicación de la organización.
- 4.16 SGSI:** Sistema de Gestión de Seguridad de la Información
- 4.17 Software:** Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de cómputo.
- 4.18 Soporte Técnico:** (Mesa de Ayuda) Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo o equipos de oficina dentro de la organización.
- 4.19 Virtualización:** En un entorno de trabajo informático donde todos los programas, aplicaciones, procesos y datos se almacenan y ejecutan centralmente, permitiendo a los usuarios acceder de forma remota a sus escritorio y/o aplicaciones desde cualquier dispositivo capaz de conectarse remotamente a estos, tales como un portátil, un PC, smartphone o cliente ligero.
- 4.20 Virus Informático:** Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador.

## 5. CONDICIONES GENERALES

Brindar a los usuarios de tecnología de la información de Team Foods y sus Filiales, un conjunto de lineamientos e instrucciones que permiten garantizar la seguridad en el ambiente informático, la información y demás recursos tecnológicos.

- Promover el uso de las mejores prácticas de seguridad informática en el trabajo, para que los usuarios colaboren con la protección de la información y recursos institucionales.
- Proponer los mecanismos de seguridad lógica, en el ambiente informático de modo que se contribuya con la confidencialidad, integridad y disponibilidad de la información.
- Regular el cumplimiento de aspectos legales y técnicos en materia de seguridad informática.

## 6. DIRECTRICES

### POLITICA DE SEGURIDAD

Las políticas y normas dadas en este documento sirven como referencia, en ningún momento pretenden ser absolutas, las mismas están sujetas a cambios en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

Toda persona natural o jurídica que utilice o intervenga con los servicios que ofrece Tecnología de la Información deberá conocer y aceptar la Política de Seguridad vigente; el desconocimiento de la misma, no exonera de responsabilidad a ningún tipo de persona, ante cualquier eventualidad que involucre la seguridad de la información de la Organización.

La Gerencia de Tecnología de la Información está conformada por:

- Dos Coordinaciones corporativas que son Coordinación de **Aplicaciones y Arquitectura de Datos TI** y Coordinación de **Operaciones TI**
- Dos coordinaciones locales, en Chile y Mexico
- Un ingeniero de Proyectos T.I.

que en conjunto se encargan de brindar servicio al usuario, y para apalancar sus responsabilidades cada coordinación debe generar y mantener las políticas y procedimientos actualizados que busquen asegurar su campo de acción.

A continuación se describen las directrices de Seguridad Informática agrupadas por campo de acción:

## 6.1 Equipos

### [De la instalación de equipos de Cómputo]

6.1.1 Todo equipo de cómputo (Servidores, Computadores de Escritorio, Portátiles, estaciones de trabajo, Dispositivos de Red), que esté o sea conectado a la Red de Team o aquel que en forma autónoma se tenga y que sea propiedad de la Organización debe de sujetarse a las normas y procedimientos de instalación que emite la Gerencia de Tecnología de la Información y particularmente la Coordinación de Operaciones T.I.

6.1.2 La **Coordinación de Operaciones T.I.** deberá tener un inventario actualizado de todos los equipos de cómputo que son propiedad de Team Foods.

6.1.3 Todo equipo de cómputo que pertenezca a la Organización que sea de propósito específico y de misión crítica, requiere estar ubicado en un área que cumpla con los requerimientos de seguridad física, condiciones ambientales y alimentación eléctrica adecuados para el correcto funcionamiento de este.

6.1.4 Todos los movimientos, reubicaciones, reasignaciones, y todo aquello que implique cambios a los equipos de cómputo de la Organización es responsabilidad de la **Coordinación de Operaciones T.I.** en conjunto con los responsables de las áreas que los soliciten y se debe cumplir con todas las normas de instalación y adecuación de los espacios para el correcto funcionamiento de los equipos.

6.1.5 La protección física de los equipos corresponde a quienes en un principio se les asigna, y se debe notificar los movimientos en caso de que existan a la **Coordinación de Operaciones T.I.**

### [Del mantenimiento de equipos de cómputo]

6.1.6 Todo lo relacionado con el mantenimiento preventivo y correctivo de los equipos de computo, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar es responsabilidad de la **Coordinación de Operaciones T.I.** que para tal fin emite las normas y procedimientos respectivos y no deben ser ejecutadas por ningún usuario.

6.1.7 El personal de soporte Técnico o Mesa de Ayuda se registrará bajo las normas y procedimientos establecidos por la **Coordinación de Operaciones T.I.**

6.1.8 Corresponde a la **Coordinación de Operaciones T.I.** dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento preventivo y /o correctivos básicos.

6.1.9 Queda prohibido dar mantenimiento a equipos de cómputo que no sean propiedad de la organización.

### [De la actualización del equipo]

6.1.10 Todo el equipo de cómputo que sea propiedad de la organización se debe procurar que sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

### [De la reubicación de equipos de Cómputo]

6.1.11 La reubicación del equipo de cómputo debe satisfacer las normas y procedimientos que la **Coordinación de Operaciones T.I.** emita para ello.

6.1.12 La reubicación de equipo de cómputo es exclusiva para equipos que pertenecen a la organización y se debé hacerce únicamente bajo la autorización de la **Coordinación de Operaciones T.I.** y del responsable del equipo contando con que la ubicación donde se va a trasladar el equipo cumpla con los medios necesarios para la instalación del equipo. Esta labor debe ser ejecutada por el personal de Soporte en Sitio o Mesa de Ayuda.

## 6.2 Control de Acceso

### [Del control de acceso al equipo de cómputo]

6.2.1 Cada equipo que entregue el área de Tecnología de la Información es asignado a un responsable, por lo que es de su competencia hacer buen uso del mismo.

6.2.2 Todo equipo tiene un único usuario asignado por lo tanto el acceso es exclusivamente para esta persona y el personal de soporte técnico.

6.2.3 Todo acceso local a equipos de cómputo con un propósito general como en el caso de los servidores de misión crítica es exclusivo al personal de Tecnología de la Información, que es autorizado por la Gerencia de Tecnología de la Información y que esta dada por el alcance del cargo.

6.2.4 Para el caso especial que se requiera el acceso local a Proveedores, Terceros o Personal de apoyo a equipos de Misión Crítica este debe estar autorizado por la **Coordinación de Operaciones T.I** o Coordinación Local de cada país y con el completo acompañamiento de un funcionario del área de Tecnología de la Información quien verificara todas las actividades que este realice.

6.2.5 Todos los accesos de manera local o presencial sobre un equipo de misión crítica debe ser registrado por el personal de Tecnología de la Información que haya sido autorizado por la Gerencia de Tecnología de la Información y es deber del funcionario autorizado verificar el correcto funcionamiento después de la finalización del trabajo realizado. **[Del control de acceso remoto]**

6.2.6 Todo acceso de manera Remota a equipos de cómputo con un propósito general como en el caso de los servidores de misión crítica es exclusivo al personal de Tecnología de la Información que es autorizado por la Gerencia de Tecnología de la Información.

6.2.8 Para el caso especial que se requiera el acceso Remoto de Proveedores, Terceros o Personal de apoyo a equipos de Misión Crítica este debe estar autorizado por la Gerencia de Tecnología de la Información y con el completo acompañamiento de un funcionario del área de Tecnología de la Información quien verifica todas las actividades que este realice.

6.2.9 Todo acceso de manera Remota a un equipo de misión crítica debe ser registrado por el personal de Tecnología de la Información que haya sido autorizado por la Gerencia de Tecnología de la Información y es deber del funcionario autorizado verificar el correcto funcionamiento después de la finalización del trabajo realizado.

6.2.10 Todo Acceso Remoto que se autorice a personal de Tecnología de Información, Proveedor. Tercero o Personal de Apoyo debe firmar la carta de entrega con el compromiso de cumplir las Políticas y Procedimientos de Tecnología de la Información.

#### **[Del control de acceso local a la red]**

6.2.11 El área de Tecnología de la Información es la responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

6.2.12 El área de Tecnología de la Información es la responsable de difundir la Normatividad y Políticas para el acceso y uso de la red y de velar por su cumplimiento.

6.2.13 El acceso a la Red de Team es exclusivo a equipos que sean propiedad de la Organización.

6.2.14 Todo equipo de cómputo que esté o sea conectado a la Red de Team debe tener las Actualizaciones de Seguridad del Sistema Operativo y del Antivirus al día.

6.2.15 No está permitido la conexión a la red de Team de equipos personales.

6.2.16 Para equipos de Personal externo con lugar de Trabajo en alguna de las sedes de Team, El área de Tecnología de la Información otorga el acceso a través de redes segmentadas que los aíslan de las Red Corporativa. Estos equipos deben cumplir con Toda la normatividad que Team emite a los equipos de la Organización.

6.2.17 Para equipos de Visitantes, El área de Tecnología de la Información otorga el acceso únicamente a través de los portales de conexión inalámbrica destinados para este fin, los cuales están aislados de la Red Corporativa y tienen acceso solo a Internet.

#### **[Del control de acceso a los Centros de Cableado]**

6.2.18 Los Centros de Cableado están ubicados en las plantas Bogotá, Oficina Central, Maipú, Morelia, DF, Caloto, Barranquilla y Buga donde se ubican los servidores de Dominio, Nice, copias de Seguridad Fastbask, Rack de cableado de Voz/Datos, Equipos de Comunicaciones, aire acondicionado y UPS's. Los Centros de Cableado hacen parte integral de los sistemas de información de la compañía, sus componentes son críticos para los diferentes procesos de la organización y por está razón se encuentran en un lugar restringido. La administración de los Centros de Cableados está a cargo de la **Coordinación de Operaciones T.I**, y Coordinaciones Locales, los cuales deben velar por la seguridad, continuidad y disponibilidad de los equipos y servicios ubicados en el Centro de Cableado.

6.2.19 El control de acceso a los centros de cableado es administrado por el área de Seguridad Física. la **Coordinación de Operaciones T.I**, y Coordinaciones Locales son responsables de verificar con el área de Seguridad Física cuales usuarios o personas de la compañía tienen acceso a estos centros de cableado. **Los proveedores de TI no cuentan con acceso al centro**

de cableado, su ingreso debe estar autorizado y realizarse en compañía de uno de los colaboradores del área de Tecnología de la Información, este debe diligenciar una bitácora de ingreso al centro

### **[Del control de acceso al Data Center de Producción y Data Center Alterno]**

6.2.20 Los Sistemas de Información críticos se encuentran ubicados en el Data Center de Producción, y su espejo en el Data Center Alterno, cuyo administración esta a cargo del proveedor del servicio.

6.2.21 El acceso físico a los Data Center esta dado de acuerdo a las políticas y procedimientos del proveedor del servicio.

6.2.22 Para el acceso de los servidores de misión crítica ubicados en estos Data Centers aplican las Políticas de Control de Acceso Remoto mencionadas anteriormente.

### **[De los Usuarios y contraseñas]**

6.2.23 Todas las cuentas de usuario, credenciales de acceso, login y contraseñas de los Sistemas de Información con los que cuenta la organización son entregados por el área de Tecnología de la Información a un único responsable, por lo que es de su competencia hacer buen uso del mismo.

6.2.24 Todos los sistemas de información, aplicaciones, equipos, accesos internos externos ó remotos que sean entregados por el área de Tecnología de la Información deben tener un sistema de autenticación que garantice la seguridad del mismo.

6.2.25 Para todos los accesos a equipos de cómputo con un propósito general como en el caso de los servidores de misión crítica se debe tener un sistema de autenticación que permita garantizar la seguridad sobre el equipo, las aplicaciones y los cambios que se puedan dar por el acceso a este tipo de equipos.

6.2.26 Las contraseñas de usuario de los Sistemas de Información, Aplicativos y equipos de cómputo que son entregados por el área de Tecnología de la Información deben cumplir con las siguientes configuraciones de Seguridad.

6.2.26.1 Las contraseñas se deben bloquear por el ingreso erróneo de está tres veces.

6.2.26.2 La contraseña de usuario tiene un periodo de vigencia de 30 días para el cambio.

6.2.26.3 La contraseña debe ser diferente de las 10 últimas.

6.2.26.4 La contraseña debe tener una longitud mínima de 8 caracteres y complejidad para ser efectiva esto quiere decir que se recomienda la combinación de mayúsculas, minúsculas, números y símbolos.

6.2.26.5 Para las contraseñas de la plataforma ISeries adicionalmente no debe permitir dígitos adyacentes.

6.2.26.6 Las contraseñas iniciales entregadas por tecnología de información deben ser cambiadas al primer ingreso por parte del usuario.

6.2.26.7 Para algunas aplicaciones donde no se cumplan a cabalidad las configuración de seguridad de contraseña se deben documentar como excepciones en el procedimiento TE-TEI-PR-012 Administración Cuentas de Usuario, previa autorización de la Gerencia de Tecnología de la Información.

6.2.26.8 La administración de Contraseñas Críticas: Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como de instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. Esta a cargo del área de T.I. del Ingeniero de Comunicaciones y Seguridad T.I. el definir y asegurar el cumplimiento del procedimiento para las contraseñas críticas.

6.2.27 Solo en casos especiales y con autorización previa de la Gerencia de Tecnología de la Información se entregará a proveedores, Terceros o Personal de Apoyo al área de Tecnología de la Información los usuarios, credencial de acceso, login y contraseñas con privilegios de Administrador a los sistemas de información y equipos de misión crítica para ejecutar una labor específica. Al finalizar esta labor estas contraseñas se deben cambiar.

6.2.28 Para las cuentas de iSeries que no ingresen en un periodo de 60 días el sistema automáticamente inactiva la cuenta

6.2.29 Las contraseñas de las aplicaciones deben estar configuradas en el Directorio Activo. Las aplicaciones que no cumplan esta directriz se deben documentar como excepción en el procedimiento TE-TEI-PR-012 Administración Cuentas de Usuario.

### **[Del control de acceso a los dispositivos]**

6.2.30 El volumen de tráfico de información en la red interna y a través de Internet hacia los servidores es

monitoreada por la Coordinación de Infraestructura y Seguridad de T.I..

6.2.31 La Coordinación de Infraestructura y Seguridad de T.I. establece controles y políticas a nivel de red con el fin de mitigar el riesgo de fuga de información crítica y sensible de la organización fuera de la red de Team.

### 6.3 Software y Aplicaciones

#### [De la adquisición de software y Aplicaciones]

6.3.1 Para cualquier adquisición de software o aplicación para ser utilizado en Team Foods o sus filiales debe tener aprobación por parte de la Gerencia de Tecnología de la Información.

6.3.2 El área de Tecnología de la Información adquirirá y utilizará software únicamente de fuentes confiables, cualquier uso de software libre debe ser autorizado por parte la Gerencia de Tecnología de la Información.

6.3.3 Todo el software o Aplicación comercial que utilice la Organización, deberá estar legalmente registrado, en los contratos de licenciamiento de software y con sus respectivas licencias.

6.3.4 Todo el software y aplicaciones de carácter comercial y libre son propiedad intelectual exclusiva de sus desarrolladores, la Organización respeta la propiedad intelectual y se rige por los contratos de licencia de sus autores.

6.3.5 La Organización, se reserva el derecho de respaldo, a cualquier funcionario, ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.

6.3.6 Todo el software y aplicaciones de carácter comercial y libre que sea utilizado por Proveedores o Terceros para desarrollos o trabajos para la Organización debe cumplir con los derechos de propiedad intelectual y contar con sus respectivas licencias, y demostrar ante la Gerencia de Tecnología de Información esta legalidad.

#### [De la instalación de Software o Aplicaciones.]

6.3.7 Es responsabilidad del área de Tecnología de la Información emitir las normas, procedimientos y manuales para la instalación del Software y Aplicaciones para los equipo de computo de la organización.

6.3.8 Para todo equipo que pertenezca a la Organización únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

6.3.9 Únicamente la Gerencia de Tecnología de la Información a través del personal que esta autorice podrán realizar instalación de software o aplicaciones, así mismo como la supervisión y asesoría de la mismo.

6.3.10 No está permitida la instalación de software o aplicaciones que puedan poner en riesgo los recursos de la Organización.

6.3.11 Con el propósito de proteger y mantener la completa integridad de los sistemas de información es imprescindible que todos y cada uno de los equipos de la Organización cuenten con el software de seguridad (Actualizaciones, Antivirus, privilegios de acceso, y todos aquellos mecanismos que brinden seguridad al equipo y a la Organización).

6.3.12 Ningún usuario puede instalar Software o Aplicación en los equipos de la Organización, esta labor es solo realizada por el área de Tecnología de la Información o a quién esta autorice.

6.3.13 Todo Software y Aplicación que es adquirido por la Organización es legal y no puede ser instalado en equipos personales ni tampoco se deben usar las licencias o contratos que son propiedad de la Organización.

6.3.14 La adquisición de software o aplicaciones por parte del personal que labore en la organización, no expresa el consentimiento de la organización, la instalación del mismo no está permitida y no garantiza ningún tipo de responsabilidad alguna para la Organización.

6.3.15 Todo software y Aplicación licenciado a la organización, es propiedad exclusiva de esta, la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

#### [De la Actualización de Software o Aplicaciones.]

6.3.16 Es responsabilidad de las Coordinaciones corporativas del área de Tecnología de la Información emitir las normas, procedimientos y manuales para la Actualización del Software y aplicaciones básico para cualquier tipo de equipo.

6.3.17 Corresponde a la Gerencia de Tecnología de la Información adquirir y autorizar cualquier adquisición y actualización del software o aplicaciones.

### 6.4. ACCESO A INTERNET

#### [Generalidades de Uso]

6.4.1 Está estrictamente prohibido cualquier uso de internet con fines políticos, particulares o cualquier otro que no sea el laboral que dio origen a la habilitación del servicio.

6.4.2 La navegación a internet debe ser única y exclusiva para consultas. **Si por sus funciones un usuario requiere de un manejo transaccional en páginas web esta deberá ser autorizada por la Gerencia de Tecnología de la Información.**

6.4.3 Todo funcionario que utilice un Recursos Informático, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

**6.4.4 Está prohibido utilizar servidores públicos de almacenamiento, servicios de correo o chat diferentes a los corporativos para almacenar, publicar o transferir información clasificada como confidencial o crítica.**

6.4.5 Todo usuario deberá comunicar al área de Tecnología de la Información cualquier incumplimiento que observe a estas normas.

6.4.6 Queda expresamente prohibido congestionar intencionalmente enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.

## 6.5. CLASIFICACIÓN DE LA INFORMACIÓN

### [De la clasificación de la Información]

6.5.1. El objetivo de la clasificación es asegurar un nivel de protección adecuado a los activos de la información. La información debe clasificarse para indicar la necesidad, prioridades y grado de protección que requiere.

6.5.2 La información tiene grados variables de sensibilidad y criticidad. Algunos elementos de información pueden requerir un nivel adicional de protección o un uso especial.

**6.5.3 La información debe clasificarse en función de su valor o importancia, requisitos legales, sensibilidad y criticidad para la organización, etc.**

6.5.4 Las clasificaciones de información y otros controles de protección asociados deberían tener en cuenta que el negocio necesita compartir o restringir la información, así como los impactos en la organización asociados a esas necesidades.

6.5.5 Las guías de clasificación deben incluir convenciones para la clasificación inicial y la reclasificación a través del tiempo, en concordancia con algunas políticas de control predeterminadas.

**6.5.6 Debe ser responsabilidad del propietario/responsable del activo definir la clasificación de este, revisarlo periódicamente y asegurarse que está actualizado y en un nivel apropiado.**

6.5.7 El nivel de protección puede ser determinado analizando la confidencialidad, integridad y disponibilidad u otro requisito para la información considerada

## 6.6. VIRTUALIZACIÓN

### [Sobre la virtualización]

6.6.1 La responsabilidad del buen uso del acceso y contraseña para la virtualización es del usuario.

6.6.2 Todo usuario que trabaje con virtualización debe mantener toda la información de la compañía en la virtualización. Dentro del computador personal, portátil u otro dispositivo con el que se conecte a la virtualización no debe almacenar información de la compañía.

6.6.3 Todo empleado de Team que vaya a trabajar en Virtualización podrá seleccionar entre dos modelos de adquisición de equipos Modelo Team o Modelo Empleado.

6.6.4 Las condiciones para la asignación de equipo a los usuarios con virtualización se establecen en el Reglamento de Asignación de Equipo Usuarios Virtualizados, el cual debe ser leído, entendido y aceptado por los empleados previamente para poder acceder a los servicios de virtualización.

**6.6.5 Modelo Team:** En este modelo Team le suministrará al empleado un equipo estandar para su uso dentro de la organización,

6.6.5.1 El equipo Modelo Team no tendrá ningún tipo de software diferente al autorizado que consistirá en el sistema operativo Windows, un navegador y las herramientas de Windows necesarias para tener acceso a la virtualización.

6.6.5.2 La adquisición y propiedad del equipo Modelo Team están a cargo de Team.

6.6.5.3 La actualización y renovación del equipo Modelo Team está a cargo de Team y realiza en el tiempo que Team considere necesario.

6.6.5.4 En los equipos de Team no se instalará ningún software adicional sin el Vo.Bo. de Tecnología de la Información.



6.6.5.5 El empleado es responsable del buen uso y cuidado de la herramienta de trabajo entregada por Team.

**6.6.6. Modelo Empleado:** En este modelo el usuario puede usar o adquirir su equipo para conectarse a la virtualización.

6.6.6.1 El equipo Modelo Empleado tendrá las herramientas de necesarias para tener acceso a la virtualización que serán entregadas por Tecnología de la Información.

6.6.5.2 La propiedad del equipo Modelo Empleado es del colaborador.

6.6.5.3 La actualización y renovación del equipo Modelo Empleado esta a cargo del empleado, quien debe procurar tener su software licenciado.

6.6.5.4 En los equipos de Modelo Empleado el usuario podrá hacer cambio o renovación bajo su responsabilidad e inversión. La instalación no depende de Team.

6.6.5.5 El empleado es responsable del buen uso y cuidado de su herramienta de trabajo

## 7. ANEXOS

### 8. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión	Fecha	Descripción resumida del cambio
2		se relaizaro cambios en el Contenido donde incluyen las politicas para la virtulización

Creado Por	Editado Por	Revisado Por	En Prueba	Aprobado Por
JUAN CARLOS MONDRAGON RIOS ASISTENTE DE ABASTECIMIENTO MP	JOSE GONZALO VACCA SANCHEZ	GENITH GODOY RINCON MANUEL JESUS SANCHEZ GOYES		ELISA SOTOMONTE OTALORA

LORENA MARGARITA IGLESIAS REDONDO @ 2016-09-02, 18:29:12