POLÍTICAS CORPORATIVAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

Presentar los elementos propios de la seguridad de la información para el obligatorio cumplimiento por parte de los colaboradores y contratistas de ComWare S.A.

2. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

2.1. Políticas de seguridad de la información.

2.1.1. Enunciado de la Política de Seguridad de la Información

"En ComWare la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, por eso nos comprometemos a preservar la confidencialidad, integridad y disponibilidad de la información de la compañía y de nuestros clientes, dando cumplimiento a los objetivos estratégicos, requisitos normativos, legales y contractuales aplicables, a través del Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo el desarrollo de estrategias de mejora continua".

2.1.1.1. Actualización. Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la Información corporativa.

2.1.1.2. Auditoría. El proceso de Gestión HSEQ debe diseñar, programar y realizar los programas de auditoría del Sistema de Gestión de Seguridad de la Información.

2.1.1.3. Adquisición de aplicativo o software. Todo aplicativo informático o software debe ser comprado o aprobado por la Gerencia de Sistemas de Información o de Infraestructura y Data Center en concordancia con las políticas y procedimientos establecidos de adquisición de bienes.

2.1.1.4. Requisito de conexión. Se debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea necesaria para la conexión a otras redes en outsourcing o de terceros.

2.1.1.5. Conexión remota. La conexión remota a la red de área local de ComWare S.A. debe realizarse a través de una conexión VPN segura suministrada por la empresa, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice la Gerencia de Infraestructura y Data Center y/o la Gerencia de Sistemas de Información.

2.1.1.6. Uso de conexiones remotas

ComWare S.A. establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la compañía; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

2.1.1.6.1. La Gerencia de Infraestructura y Data Center debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica del ComWare S.A.
2.1.1.6.2. La Gerencia de Infraestructura y Data Center debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

2.1.1.6.3. La Gerencia de Infraestructura y Data Center debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica del ComWare S.A. manera permanente.

2.1.1.6.4. Los Colaboradores que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la ComWare y deben acatar las políticas o lineamientos de uso establecidas para dichas conexiones.

2.1.1.6.5. Los Colaboradores únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.

2.1.1.7. Responsabilidad cumplimiento de protocolos de seguridad. Los Vicepresidentes, Líderes de Proceso y los Gerentes de Proyectos deben asegurarse de que se cumplan todos los procedimientos de seguridad de la información dentro de su proceso o proyecto, de acuerdo con lo establecido en el presente documento.

2.1.1.8. Intercambio de información. Cuando se requiera intercambio de información y/o envío de información de la Compañía a un tercero, la transferencia debe hacerse utilizando protocolos seguros y a través de plataformas corporativas.

2.1.1.9. Comité de Seguridad. La Compañía debe establecer un Comité de Seguridad de la Información compuesto por:

a) El Vicepresidente de Servicios y Operaciones (quien lo presidirá).
b) El Gerente de Infraestructura (quien hará las veces de secretario).
c) El Gerente de Sistemas de Información (quien hará las veces de secretario)
d) El Gerente de Asuntos Legales.
e) El Director HSEQ.
f) El Gerente de la PMO.
g) El Responsable de Seguridad de la Información o quien haga sus veces.

2.1.1.9.1. Dicho Comité se reunirá como mínimo cada 3 meses, para revisar la consistencia y vigencia del presente documento así como para discutir asuntos estratégicos de la Seguridad de la Información Corporativa, las funciones específicas del comité se detallan en el manual del sistema de seguridad de la información.

2.1.1.9.2. Adicionalmente dicho Comité definirá de acuerdo a la clasificación de la información, qué datos deben ser cifrados y dará las directrices necesarias para la implementación de los respectivos controles (dispositivos a emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

2.1.2. Política de clasificación de la información.

2.1.2.1 Definición de Información: Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Compañía.

2.1.2.1.1 Para ComWare S.A., la información es un activo y por consiguiente se deben establecer todos los mecanismos necesarios y suficientes para protegerla y darle el uso adecuado. Lo anterior de acuerdo al marco legal establecido por la ley colombiana y a las políticas internas que en relación a esta materia ha establecido la Compañía.

2.1.2.1.2. Esta Política tiene por objeto establecer los principios, bases, lineamientos, procedimientos y normas necesarios para proteger la información y documentación sensible de la Compañía, así como del conocimiento y divulgación a personas naturales o jurídicas no autorizadas.

2.1.2.2 Niveles de Clasificación.

Es responsabilidad de cada uno de los colaboradores de la Compañía que al momento de generar información, establezcan el nivel de clasificación para la misma de acuerdo con al menos uno de los criterios establecidos para tal fin.

Para ComWare S.A., la información se puede clasificar en uno de los siguientes niveles:

2.1.2.2.1 Clasificación de la información por su contenido:

2.1.2.2.1.1. Altamente Secreta: Se aplicará a la información cuya divulgación no autorizada podría razonablemente esperarse que cause daños excepcionalmente graves a la Compañía.

2.1.2.2.1.2. Secreto: Se refiere a la información cuya divulgación no autorizada podría razonablemente esperarse que cause daños graves a la Compañía o a una oportunidad de negocio.

2.1.2.2.1.3. Confidencial: Se aplicará a la información que podría causar daños a la Compañía o a la oportunidad de negocio.

2.1.2.2.1.4. Público: Se refiere a toda la información que no está clasificada en ninguno de los niveles anteriores.

2.1.2.2.2 Clasificación de la información por su audiencia:

2.1.2.2.2.1. Tipo 1: Información clasifica como Altamente Secreto disponible únicamente para los socios de la Compañía.

2.1.2.2.2.2. Tipo 2: Información clasificada como secreto disponible únicamente para los miembros del Comité de Gerencia de la Compañía (Presidente, Vicepresidente y Gerentes de nivel 1) y

Gerentes de nivel 2 o Directores (colaboradores con cargo de Gerente o Director que reportan a una Vicepresidencia).

2.1.2.2.2.3. General: Información clasificada como Confidencial o Pública de acceso General a los colaboradores de la Organización.

PARÁGRAFO: El DLP –Data Loss Prevention de la Compañía enfocará su monitoreo principalmente en información clasificada como Secreta, Altamente Secreta, Tipo 1, Tipo 2 y/o Tipo3.Es responsabilidad del colaborador al momento de generar la información, la correcta clasificación de la misma de acuerdo con los niveles arriba descritos.

2.1.3. Políticas de seguridad para gestión humana

2.1.3.1 Aseguramiento de la información por parte de los colaboradores: Se debe asegurar que los colaboradores, contratistas y demás colaboradores de la Compañía entiendan y acepten sus responsabilidades en relación con las políticas de seguridad de la información y lo definido por la ley para información sensible y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información corporativa y de dato personal frente a terceros y frente a los mismos colaboradores y/o contratistas.

2.1.4. Políticas específicas para usuarios.

2.1.4.1 Licencia. Todo el software usado en la plataforma tecnológica de la Compañía debe tener su respectiva licencia proveniente de una adquisición formal por parte de la Empresa y estar acorde con los derechos de autor.

2.1.4.1.1 Los colaboradores no podrán utilizar usuarios genéricos para la instalación de aplicaciones, sistemas de información o plataformas de información licenciadas

2.1.4.2 Copias. La Compañía instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades.

2.1.4.3 Prohibición uso de programas sin licencia. El uso de programas sin la respectiva licencia y autorización de la Compañía (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la Empresa, por lo que ésta práctica no está autorizada y quedarán sujetos a las acciones disciplinarias establecidas por la Compañía o las sanciones que especifique la ley.

2.1.4.4 Responsabilidad del colaborador por la instalación de un programa sin autorización: La Compañía no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus colaboradores o contratistas. Al respecto, implementará mecanismos tecnológicos para evitar que esto pase, sin embargo, la responsabilidad por el software instalado en los equipos de los colaboradores y/o contratistas, es de estos últimos.

2.1.4.5 Aprobación para utilizar dispositivos de almacenamiento externo. El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas,

celulares, etc.) puede ocasionalmente generar riesgos para la Empresa al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal de la Gerencia de infraestructura de data center de la Compañía, previa solicitud escrita por parte del jefe inmediato.

2.1.4.6 Propiedad de software: Al momento de adquirir una licencia de software, la Compañía adquiere el derecho de uso de la misma de acuerdo con los términos y condiciones que el fabricante establezca para tal fin.

2.1.4.7 Copias no autorizadas de Software. La copia no autorizada de software o de su documentación, implica una violación a la política general de la Empresa. Aquellos colaboradores, contratistas o demás colaboradores que utilicen copias no autorizadas de software o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por la Compañía o las sanciones que especifique la ley.

2.1.4.8 Control de copias no autorizadas de Software. La Compañía ejercerá el derecho de proteger su buen nombre y sus inversiones en hardware y software, implantando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la Empresa. Estos controles harán valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.

2.1.4.8.1. El uso de los recursos tecnológicos y de software asignados a los colaboradores de la Compañía son responsabilidad de cada colaborador.

2.1.4.9 Almacenamiento en la Nube: La Compañía suministrará una cuota de almacenamiento de la información en una plataforma en la Nube administrada por un tercero con los permisos necesarios para que cada usuario guarde la información digital clasificada o corporativa y sobre ella se garantizará la disponibilidad, lo anterior de acuerdo con lo establecido en el documento de Políticas de almacenamiento en la nube, el cual es presentado más adelante en este documento.

2.1.4.9.1. Es responsabilidad de cada colaborador dueño de la información u custodio de la información, asegurar el control de acceso únicamente a las personas interesadas o autorizadas.

2.1.4.10 Responsables de la información. Los usuarios son los responsables de la información que administran en sus equipos y deben abstenerse de almacenar en ellos información no corporativa.

2.1.4.10.1. Los usuarios sólo tendrán acceso a la información y recursos autorizados por la Compañía y conforme a su rol o cargo, adicionalmente serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

2.1.4.10.2. Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, teléfonos celulares, Tablet, escáner, etc.) sólo deben utilizarse para los fines autorizados por la Empresa y propios con su razón de ser como Compañía.

2.1.4.10.3. Cualquier evento o posible incidente que afecte la confidencialidad, integridad y disponibilidad de la información, debe ser reportado inmediatamente al Service Desk, a través de los procesos establecidos para tal fin. (TI-SVD-PR-07 Procedimiento Gestión de Incidentes de Seguridad de la Información).

2.1.4.11. Confidencialidad de la información. Los colaboradores de la compañía se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones y de acuerdo al nivel de clasificación establecido por la compañía. En consecuencia, se obligan a mantenerla de manera confidencial, privada, y a protegerla para evitar su divulgación indebida, pérdida o fuga de información.

2.1.4.11.1. **Prohibición en la utilización de la información.** Los colaboradores de la Empresa no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.

2.1.4.11.2. Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) sólo deben utilizarse para los fines autorizados por la Empresa y propios con su razón de ser como Compañía.

2.1.4.12 Concientización sobre el manejo de la información. Los Vicepresidentes, Gerentes y Directores de los diferentes procesos de la Compañía, en conjunto con el Comité de Seguridad de la Información propiciarán actividades para concientizar al personal sobre las precauciones necesarias que deben tener los usuarios finales a fin de evitar revelar información confidencial cuando se hace una llamada telefónica, que pueda ser interceptada mediante acceso físico a la línea o ser escuchada por personas que se encuentren cerca. Lo anterior debe aplicar también cuando el colaborador se encuentre en sitios y transporte públicos, áreas comunes dentro de la compañía.

2.1.4.12.1. Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados.

2.1.5. Políticas específicas para empleados y contratistas de las Gerencias de Infraestructura de Data Center y Sistemas de información.

2.1.5.1 Manejo de la clave. El personal de la Gerencia de sistemas de información no puede dar a conocer su clave de usuario y/o de administración de los diferentes sistemas a terceros sin previa autorización del gerente de infraestructura y data center.

2.1.5.1.1. Los usuarios y claves de los administradores de sistemas son de uso personal e intransferible.

2.1.5.1.2. El personal debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la Empresa de acuerdo al rol asignado.

2.1.5.1.3. Los administradores de los sistemas deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Gerente de Infraestructura de Data Center.

2.1.5.1.4. Para el cambio o retiro de equipos de colaboradores, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la Empresa.

2.1.5.1.5. Los colaboradores encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado por la Gerencia de Infraestructura de Data Center.

2.1.5.1.6. Los administradores y/o colaboradores que operen o administren sistemas de información, aplicaciones, bases de datos y plataformas no podrán utilizar los usuarios de dominio propios para la instalación de los mismos, se debe solicitar a la gerencia de infraestructura un usuario de dominio asignado exclusivamente a la plataforma, sistemas de información, aplicaciones, bases de datos y plataformas

2.1.5.2 Privilegios. Los colaboradores de la Gerencia de Sistemas de información no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Gerente de Infraestructura de Data Center o sistemas de información, siguiendo el procedimiento que para tal fin se establezca en el Service Desk.

2.1.5.2.1. Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.

2.1.5.2.2. Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la Empresa. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la Empresa.

2.1.5.2.3 La copia de programas o documentación, requiere tener la aprobación escrita de la Compañía y del proveedor si éste lo exige.

2.1.5.2.4. Los colaboradores de la Gerencia de Sistemas de Información deben velar porque se cumpla con el registro en la bitácora de acceso al datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por la Gerencia del área o por quien esta delegue.

2.1.5.2.5. Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado explícitamente por la Empresa a través del Comité de Seguridad de la Información.

2.1.5.2.6 El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado explícitamente.

2.1.5.**2.7** Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

2.1.5.2.8 Las pruebas de laboratorio o pilotos deben ser autorizadas por la Gerencia de Infraestructura de datacenter o Sistemas de información, para sistemas de información, de software tipo freeware o shareware o de sistemas que necesiten conexión a internet; estas deben ser realizadas sin conexión a la red LAN de la Empresa y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción.

2.1.5.3 Políticas específicas para el Webmaster de la Compañía, quien hace parte de la Gerencia de Mercadeo y cumple con las políticas y procedimientos definidos por la Gerencia de sistemas de información.

2.1.5.3.1. Los responsables de los contenidos de las páginas Web (Webmasters o sites), deben preparar y depurar la información de su proceso o proyecto y reportar al Service Desk los requerimientos de actualización de la versión del software; deben disponer de un archivo actualizado

con la información de la página inicial del sitio; y deben registrar la autorización de publicación por parte del colaborador autorizado y coordinar con el administrador web los lineamientos del sitio.

2.1.5.3.2. Se deberá seguir la Política Editorial y Actualización de Contenidos Web, que permita auditar la publicación o modificación de información oficial en las páginas web.

2.1.5.3.3. Las claves de acceso de los responsables de los contenidos de las páginas Web (Webmasters), son estrictamente confidenciales, personales e intransferibles.

2.1.6. Política de Proveedores.

2.1.6.1 Selección de Proveedores, Se deben establecer criterios de selección que contemplen la historia y reputación de proveedores, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la Compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la Empresa.

2.1.6.2 Análisis de riesgos Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la Compañía. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de Seguridad de la Información antes de firmar el contrato de outsourcing.

2.1.6.3 Acuerdos con proveedores.

2.1.6.3.1. En los casos en que los acercamientos o acuerdos comerciales entre las partes requieran la entrega de información por parte de Comware a terceros se deberá subscribir un acuerdo de confidencialidad, o un contrato que incluya una cláusula de confidencialidad;

2.1.6.3.2. Si la información a intercambiar lo amerita teniendo en cuenta la clasificación de la misma de acuerdo a los niveles de seguridad, se debe preparar y legalizar un acuerdo de confidencialidad entre las parte de acuerdo con el objeto y alcance del contrato; el cual debe quedar firmado por ambas partes.

2.1.7. Política de retención y archivo de datos.

2.1.7.1. La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en la Compañía de acuerdo a las tablas de retención documental.

2.1.7.2. Las reglas y los principios generales que regulan la función archivística, se encuentran definidos por la Ley.

2.1.7.3. La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

2.1.8. Política de disposición de información, medios y equipos.

2.1.8.1. Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto

estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

2.1.9. Política de respaldo y restauración de información.

2.1.9.1. La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, etc.

2.1.9.2. Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, así como el DBA (Administrador de las Bases de Datos de la Empresa) son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) y el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.

2.1.9.3. Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

2.1.9.4. Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

2.1.9.5. Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

2.1.9.6. Ningún tipo de información corporativa puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin en la plataforma de almacenamiento en la nube.

2.1.9.7. La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

2.1.9.8. Semanalmente los administradores de infraestructura de la Compañía, verificarán la correcta ejecución de los procesos de backup, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.

2.1.9.9. La Gerencia de Sistemas de Información debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la Compañía.

2.1.9.10. Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

2.1.9.11. Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega La Compañía a los usuarios.

2.1.10. Política de gestión de activos de información.

2.1.10.1 Inventario de activos de información

2.1.10.1.1 La Compañía mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el responsable de seguridad de la información.

2.1.10.1.2 Una parte de los activos de información se mantendrá en una base de datos bajo la responsabilidad de la Gerencia de Infraestructura y Data Center. (Base de datos de gestión de configuraciones -Configuration Management Database CMDB).

2.1.10.2 Propietarios de los activos de información

2.1.10.2.1 La Compañía es propietaria de los activos de información y los administradores de estos activos son los colaboradores, contratistas o demás personal de la Empresa (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones (TIC).

2.1.10.2.2. Los propietarios de los activos de información, son responsables de la clasificación, etiquetado, documentación, mantenimiento y actualización del inventario de activos de información a su cargo, así como de la asignación y revisión periódica de los permisos de accesos otorgados a los colaboradores de acuerdo a sus funciones y competencias.

2.1.11. Política de uso de los activos.

2.1.11.1. Los activos de información pertenecen a la Compañía y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

2.1.11.2. Los usuarios deberán utilizar únicamente los programas y equipos autorizados por la Compañía.

2.1.11.3. La Compañía proporcionará al usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Compañía, para copiar cualquier tipo de información clasificada o sensible debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la Compañía. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Empresa, serán sancionadas de acuerdo con las normas y legislación vigentes.

2.1.11.4. Periódicamente, la Gerencia de Infraestructura de Data Center efectuará la revisión de los programas utilizados en cada proceso. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerada como una violación a las Políticas de Seguridad de la Información de la Compañía.

2.1.11.5. Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través del Service Desk y con la respectiva autorización de la Gerencia de Sistemas de Información.

2.1.11.6. Estarán bajo custodia de la Gerencia de Infraestructura de Data Center y/o sistemas de información los medios magnéticos o electrónicos (CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso. Adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.

2.1.11.7. Los recursos informáticos de la Compañía no podrán ser utilizados para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

2.1.11.8. Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Gerencia de Sistemas de Información:

a) Instalar software en cualquier equipo de la Compañía;

b) Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la Compañía;

c) Modificar, revisar, transformar o adaptar cualquier software propiedad de la Compañía;

d) Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Compañía.

e) Copiar o distribuir cualquier software de propiedad de la Compañía.

2.1.11.9. El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad o uso indebido que tenga conocimiento.

2.1.11.10. El usuario será responsable de todas las transacciones o acciones efectuadas con su cuenta de usuario.

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

2.1.11.12. Cada usuario es responsable de asegurar que el uso de redes externas, tal como Internet, no comprometa la seguridad de los recursos informáticos de la Compañía. La Gerencia de Infraestructura de Data Center es el subproceso responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la Empresa; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

2.1.11.13. Todo archivo o material recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas destructivos antes de ser instalados en la infraestructura TIC de la Compañía.

2.1.11.14. Todos los archivos provenientes de equipos externos a la Compañía, deben ser revisados para detección de virus antes de su utilización dentro de la red de la Compañía.

2.1.11.15. Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios de la Gerencia de Infraestructura de la Compañía.

2.1.11.16. La información de la Compañía debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información esté segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

2.1.12. Política de uso de almacenamiento en la nube.

2.1.12.1 Objeto: Definir los lineamientos y términos para garantizar el máximo aprovechamiento de la plataforma de almacenamiento en la nube, con el fin de garantizar la confidencialidad, integridad, disponibilidad y accesibilidad en un entorno colaborativo a la información corporativa de ComWare S.A.

2.1.12.2 Ámbito de aplicación: Serán sujetos obligados de las disposiciones contenidas en el presente todos los colaboradores de ComWare S.A. quienes en virtud de las responsabilidades propias de su cargo crean, modifican, eliminan y en general manipulan información de la Compañía.

2.1.12.3 Principios y fundamentos de almacenamiento en la nube. La solución permite eliminar las barreras físicas de tiempo y espacio y de esta manera contar con toda la información y documentos corporativos en cualquier parte. Además de poder contar con toda la información (independiente del tipo de archivo) en cualquier parte (se puede acceder también a través de dispositivos móviles) se tienen las siguientes ventajas:

2.1.12.3.1. Se puede invitar a otros usuarios a ver y descargar todos los archivos que se quiera, o se puede invitarlos para que trabajen en ellos, sin necesidad de enviar archivos adjuntos por correo electrónico.

2.1.12.3.2. Puede desarrollarse videoconferencias para en conjunto revisar los archivos con otras personas, independiente de la ubicación física de los mismos.

2.1.12.3.3. El sistema cuenta con todos los mecanismos de auditoría y control que permiten tener la tranquilidad de que, a pesar de estar en la nube, se encuentran debidamente protegidos y resguardados, por lo que ya no es necesaria la realización de actividades de backup para proteger la información.

2.1.12.4 Lineamiento uso compartido externo. La funcionalidad de compartir documentos con personas externas a la organización se encuentra restringida, para obtener los permisos necesarios se debe seguir el Instructivo de Transferencia de Información.

2.1.12.5 Gestión de almacenamiento en la nube. La implementación y administración de la plataforma de almacenamiento en la nube será liderada por la Gerencia de Infraestructura de Data center, la cual orientará al resto de procesos y a los colaboradores en general de ComWare S.A. para su ejecución, en coordinación con el Service Desk de la Compañía.

2.1.12.6 Implementación y uso del almacenamiento en la nube. Cada uno de los colaboradores de la Compañía que posea información de la empresa será el responsable de desarrollar las tareas para trasladar su información corporativa al espacio dentro de la nube asignado para tal fin. La Gerencia de Infraestructura de Data center apoyará esta actividad y proporcionará un procedimiento para la realización de esta actividad.

2.1.12.7 Manual para la implementación del almacenamiento en la nube. Para garantizar el cumplimiento de lo establecido en la presente Política, la Gerencia de Infraestructura de Data center elaborará los manuales para la implementación de para la información corporativa de ComWare S.A.

2.1.13. Política de uso de Internet.

2.1.13.1 Gestión del acceso a Internet. La implementación y administración de la plataforma tecnológica necesaria para suministrar el acceso a Internet será liderada por la Gerencia de Infraestructura de Data Center, la cual orientará al resto de procesos y a los colaboradores en general de ComWare S.A. para su adecuado uso, en coordinación con el Service Desk de la Compañía.

2.1.13.2 Implementación y uso de Internet. Cada uno de los colaboradores de la Compañía posee una credencial (usuario y contraseña) que le permite el acceso a los recursos tecnológicos y de información de la Compañía de acuerdo con el perfil de usuario y las responsabilidades propias de su cargo. Es responsabilidad de cada uno de los colaboradores de la Empresa el buen gobierno sobre esa credencial. La Gerencia de Infraestructura de Data Center monitoreará esta actividad y proporcionará procedimientos para facilitar y encauzar la realización de esta actividad.

2.1.13.2.1. Usos aceptables de Internet. El servicio de acceso a Internet se dispone para los siguientes tópicos:

a) Comunicación e intercambio de información entre empleados de la Compañía.

b) Comunicación e intercambio de información entre empleados y clientes de la Compañía.

c) Comunicación e intercambio de información entre empleados y proveedores de la Compañía.

d) Todos los anteriores siempre y cuando estén enmarcados en tareas necesarias para el cumplimiento en los fines establecidos por la misión y documentos estratégicos de la Compañía.

2.1.13.3 Usos inaceptables de Internet. No está permitido el uso de los recursos de Internet en los siguientes aspectos:

2.1.13.3.1 Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

2.1.13.3.2 Acceso a sitios web que presenten de manera explícita o implícita material pornográfico, o bien materiales ofensivos en perjuicio de terceros.

2.1.13.3.3 Acceso a sitios web relacionados con terrorismo, ciberterrorismo, armamentismo y/o internet oscuro.

2.1.13.3.4 Utilización de los servicios de correo para envío de información personal, chistes, pensamientos y cualquier otra información que no sea de carácter laboral.

2.1.13.3.5 Portales de selección y/o contratación laboral, excepto para la Gerencia de Gestión Humana.

2.1.13.4 Control de uso del servicio.

2.1.13.4.1. La Gerencia de Infraestructura de Data Center, no ejerce control sobre el contenido de la información que pase por la red, o de quien la utilice, quedando bajo la responsabilidad del colaborador que la acceda o la utilice. No obstante a lo anterior la Gerencia de Infraestructura de Data Center pondrá en funcionamiento herramientas de control que posibilitan analizar y detectar usos indebidos, por lo anterior se advierte que el contenido de la información es monitoreado y sujeto a controles y reportes sobre el uso.
2.1.13.4.2. La Gerencia de Infraestructura de Data Center no da garantías de ningún tipo, sea expresa o implícitamente, para el servicio que provee, por lo que no existirá ninguna responsabilidad por cualquier daño que el usuario sufra causado por negligencia propia o los errores u omisiones de sus usuarios.

2.1.13.4.3. Cualquiera que acceda a otras redes nacionales o internacionales por medio del servicio de acceso a Internet de la Compañía deberá acatar las reglas que rijan las mismas.

2.1.13.4.4. Corre por cuenta y riesgo del usuario cualquier información obtenida por medio del servicio de Internet.

2.1.13.4.5. Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ninguna otra empresa o institución.

2.1.13.4.6. La Gerencia de Infraestructura de Data Center tiene la autoridad para controlar y negar el acceso a cualquier colaborador que viole las políticas o interfiera con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.

2.1.13.4.7. La Gerencia de Infraestructura de Data Center utilizará herramientas de monitoreo del uso de los recursos por lo cual podrá establecer controles de acceso a sitio y de envió de información masivamente por la red.

2.1.13.4.8. La Gerencia de Infraestructura de Data Center enviará reporte del uso del servicio de correo o Internet a las Vicepresidencias respectivas para que tomen medidas tendientes a mejorar su utilización.

2.1.13.4.9. La demanda de servicios puede ocasionalmente exceder la disponibilidad, por lo que serán establecidas las prioridades, dando la más alta prioridad a las actividades consideradas las más esenciales para llevar a cabo la misión de la Compañía.

2.1.13.4.10. Los sistemas de Gestión de Eventos monitorearán en forma automática los sitios visitados por los empleados por lo cual se advierte que se aplicarán las sanciones establecidas por el acceso indebido.

2.1.13.5 Prohibiciones.

2.1.13.5.1. La transmisión de materiales en violación de cualquier regulación, queda prohibida. Esto incluye, pero no se limita a materiales con derechos de propiedad intelectual, habeas data, materiales que legalmente se consideren amenazantes u obscenos.

2.1.13.5.2. Queda prohibido el envío de información en forma masiva a todo la Compañía o Grupos de usuarios, por lo cual se restringe este uso en forma automática.

2.1.13.5.3. Para el manejo de archivos bajo plataformas de nube pública tales como "Spotify", "Dropbox", "Skydrive, "Wetransfer", etc, se requiere con la autorización respectiva de la Gerencia de Infraestructura de Data Center de la Compañía, la cual puede ser solicitada vía correo electrónico a la instancia pertinente.

2.1.13.5.4. Debido al alto nivel de seguridad con el que se debe contar en el acceso a Internet, las claves de acceso a la WEB y correo electrónico deberán de ser estrictamente confidenciales y personales. Además de censurar la visita de páginas en la red dedicadas a temas que no sean del interés o en línea con la razón de ser y objetivos corporativos de ComWare S.A., o bien que simplemente se haga mal uso de los recursos para acceder información no relacionada con el área de trabajo.

2.1.13.5.5. Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas de la Compañía.

2.1.13.5.6. Utilizar los recursos de la Compañía para lograr acceso no autorizado a redes y sistemas remotos.

2.1.13.5.7. Provocar deliberadamente el mal funcionamiento de computadores y servidores ya sea de la red corporativa de ComWare S.A. o de redes externas.

2.1.13.5.8. Monopolizar los recursos en perjuicio de los otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones voluminosas, uso de recursos de impresión no autorizado.

2.1.13.5.9. Poner información en la red que infrinja los derechos de los demás.

2.1.13.5.10. Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.

2.1.13.5.11. Utilizar los servicios de red para ver publicaciones de deportes.

2.1.13.5.12. Utilizar los servicios de red para ver publicaciones de pornografía.

2.1.13.5.13. Utilizar los servicios de red para enviar archivos que sean confidenciales.

2.1.13.5.14. La exhibición de material pornográfico en cualquier lugar de la Compañía utilizando el equipo de cómputo y/o los servicios de comunicación de la Empresa, asimismo el uso de equipo electrónico de la Empresa para observar o reproducir pornografía. El incurrir en el incumplimiento de esta normativa acarreará una falta grave que será sancionada según las regulaciones vigentes establecidas en el Reglamento Interno del Trabajo, de acuerdo con los lineamientos establecidos por el Código Sustantivo del Trabajo.

2.1.13.5.15. Envío de mensajes masivamente a todos los usuarios de la red o segmentos acerca de iniciación y facilitaciones de cadenas y creación de procesos discusión y contestación.

2.1.14. Política de uso de impresoras y del servicio de Impresión.

2.1.14.1. Los documentos que se impriman en las impresoras de la Compañía deben ser de carácter corporativo y de acuerdo con los principios y razón de ser de la Empresa.

2.1.14.2. Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión para que no se afecte su correcto funcionamiento.

2.1.14.3. Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Service Desk.

2.1.15. Política de control de Acceso

2.1.15.1. Es responsabilidad de Gestión Financiera establecer y gestionar los controles para el acceso físico, Es responsabilidad de Gestión TIC´s, establecer y gestionar los controles para el acceso de la información digital.

2.1.15.2. La Gerencia de Infraestructura y Data Center debe asegurar que las redes inalámbricas de la Compañía cuenten con métodos de autenticación que evite accesos no autorizados.
2.1.15.3. La Gerencia de Infraestructura y Data Center debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

2.1.15.4. Los colaboradores, antes de contar con acceso lógico por primera vez a la red de datos del COMWARE, deben contar con el formato de solicitud de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

2.1.15.5. COMWARE, establecerá y controlará los privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Compañía. Así mismo, velará porque los colaboradores y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y la asignación de los derechos de acceso esté regulada por procedimientos establecidos para tal fin.

2.1.15.6. Los colaboradores usuarios de los recursos tecnológicos y los sistemas de información del COMWARE, realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

2.1.15.7. La Gerencia de Infraestructura y Data Center o Sistemas de Información, velará porque los recursos de la plataforma tecnológica y los servicios de red de la compañía sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

2.1.15.8. Las Vicepresidencias, Gerencias, Direcciones o Jefaturas como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

2.1.15.9. La Gerencias de Infraestructura y Data Center o Sistemas de Información como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

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

2.1.16.1. Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no son de propiedad de la Compañía, sólo tendrán acceso Wi-Fi a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por la Compañía.

2.1.16.2. La instalación, activación y gestión de los puntos de red es responsabilidad de la Gerencia de Infraestructura y Data Center

2.1.16.3. Solo se permitirá la conexión de equipos corporativos a la red LAN de la Compañía.

2.1.16.4. El acceso a la red de datos de ComWare S.A. se realizará empleando la cuenta de dominio de red de cada usuario. El colaborador debe velar por la privacidad de sus(s) clave(s) de acceso a la red y aplicaciones, evitando comunicarla(s) a terceros, es de uso personal e intransferible. En caso de que la clave de acceso (contraseña) pudiera estar en conocimiento de terceras personas, el usuario deberá solicitar el cambio de la(s) clave(s) de manera inmediata.

2.1.16.5. Los Colaboradores utilizarán únicamente los servicios para los cuales está autorizado. No deberá usar la cuenta de otro usuario, ni intentar apoderarse de claves de acceso de otros, así como no deberá intentar acceder ni modificar archivos que no son de su alcance directo o injerencia.

2.1.17. Políticas de seguridad del centro de datos y centros de cableado.

2.1.17.1 No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

2.1.17.2. La Gerencia de Infraestructura debe garantizar que el control de acceso al centro de datos de ComWare S.A., cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.

2.1.17.3. La Gerencia de Infraestructura debe garantizar que todos los equipos de los centros de datos cuentan con un sistema alterno de respaldo de energía.

2.1.17.4. La limpieza y aseo del centro de datos estará a cargo del subproceso de Servicios Generales y debe efectuarse en presencia de un empleado o contratista de la Gerencia de Infraestructura Tecnológica de la Compañía. El personal de servicios generales debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de servicios generales con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

2.1.17.5. En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

El centro de datos debe estar provisto de:

a) Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de Seguridad y Salud en el Trabajo,

b) Pisos elaborados con materiales no combustibles.

c) Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.

d) Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.

e) Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

f) Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

2.1.17.6. El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.

2.1.17.7. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

2.1.17.8. Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un empleado o contratista autorizado de la Compañía.

2.1.17.9. Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el Colaborador responsable de la actividad se ubicará dentro del centro de datos.

2.1.17.10. Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

2.1.17.11. Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

2.1.17.12. Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

2.1.18. Políticas de seguridad de los Equipos.

2.1.18.1. Protecciones en el suministro de energía.

2.1.18.1.1. A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el subproceso de Servicios Generales.

2.1.18.2. Seguridad del cableado.

2.1.18.2.1. Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

2.1.18.2.2. Deben existir planos que describan las conexiones del cableado.

2.1.18.2.3. El acceso a los centros de cableado (Racks), debe estar protegido.

2.1.18.3. Mantenimiento de los Equipos.

2.1.18.3.1. La Compañía debe mantener contratos de soporte y mantenimiento de los equipos críticos.

2.1.18.3.2. Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.

2.1.18.3.3. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.

2.1.18.3.4. Los equipos que requieran salir de las instalaciones de la Compañía para reparación, mantenimiento o para brindar algún servicio en un Cliente, deben estar debidamente autorizados y

se debe garantizar que en dichos elementos no se encuentra información establecida como crítica en la clasificación de la información de acuerdo a los niveles de clasificación de la información.

2.1.18.3.5. Para que los equipos puedan salir fuera de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la Compañía.

2.1.18.3.6. Cuando un equipo vaya a salir de la Compañía, éste debe contar con la debida autorización de la Vicepresidencia de Servicios y Operaciones, la Gerencia de Sistemas de Información, la Gerencia de Infraestructura, la Dirección de Contabilidad y/o la Gerencia de Gestión Humana.

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

2.1.19.1. Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la Empresa de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

2.1.19.2. Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Empresa.

Los usuarios deben tener en cuenta los siguientes aspectos:

2.1.19.3. No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.

2.1.19.4. El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.

2.1.19.5. Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

2.1.19.6. Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.

2.1.19.7. La clave de acceso será desbloqueada sólo por el Service Desk, luego de la solicitud formal por parte del responsable de la cuenta. Para todas las cuentas especiales, la reactivación debe ser documentada y comunicada.

Las claves o contraseñas deben:

2.1.19.8. Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, Comware, Colombia, etc.

2.1.19.9. Tener mínimo diez caracteres alfanuméricos.

2.1.19.10. Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.

2.1.19.11. Cambiarse obligatoriamente cada 30 días, o cuando lo establezca la Gerencia de Sistemas de Información.

2.1.19.12. Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.

2.1.19.13. Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.

2.1.19.14. No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.

2.1.19.15. No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.

2.1.19.16. No ser reveladas a ninguna persona, incluyendo al personal de la Gerencia de Sistemas de Información.

2.1.19.17. No registrarlas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.

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

2.1.20.1. Los sistemas de información, aplicaciones, licencias y en general el software corporativo solo pueden ser adquiridos por la Gerencia de Sistemas de Información y/o con la aprobación explícita de este Subproceso.

2.1.20.2. En caso de desarrollos propios de la Empresa se debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa a la Empresa y que sean registrados ante la Dirección General de Derechos de Autor del Ministerio del Interior y de Justicia.

2.1.20.3. La compra de una licencia de un programa permitirá a la Compañía realizar una copia de seguridad (a no ser que esté estipulado de manera distinta), para ser utilizada en caso de que el medio se averíe.

2.1.20.4. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

2.1.20.5. La Gerencia de Sistemas de Información será la única dependencia autorizada para realizar copia de seguridad del software original.

2.1.20.6. La instalación del software en las máquinas de la Compañía, se realizará únicamente a través del Service Desk de la Compañía.

2.1.20.7. El software proporcionado por la Compañía no puede ser copiado o suministrado a terceros.

2.1.20.8. En los equipos de la Compañía se podrá utilizar el software licenciado por la Gerencia de Sistemas de Información y el adquirido o licenciado por los proyectos o áreas de la Compañía.

2.1.20.9. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Gerencia de Sistemas de Información, la cual analizará las propuestas presentadas para su evaluación y aprobación.

2.1.20.10. El software que se adquiera a través de los proyectos, debe quedar a nombre del Cliente cuando así esté definido en la propuesta de servicios. De lo contrario, quedará a nombre de ComWare S.A.

2.1.20.11. Se encuentra prohibido el uso e instalación de juegos en los computadores de la Compañía.

2.1.20.12. Para el caso del software de licenciamiento tipo freeware o shareware, incluyendo las aplicaciones tipo GNU o GPL, cuando estas se requieran y así no impliquen desembolso económico, las mismas deben seguir las políticas que se acaban de presentar.

2.1.21. Política de uso de dispositivos móviles.

2.1.21.1. De los colaboradores de ComWare:

2.1.21.1.1. Los colaboradores de ComWare deben evitar usar los dispositivos móviles corporativos (Celulares inteligentes, Portátiles, tabletas entre otros), en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

2.1.21.1.2. Los colaboradores de ComWare no deben modificar las configuraciones de seguridad de los dispositivos móviles corporativos, los cuales están bajo su responsabilidad, ni desinstalar el software provisto con ellos, al momento de su entrega.

2.1.21.1.3. Los colaboradores de ComWare que utilicen dispositivos móviles de propiedad de ComWare, deben evitar la instalación de programas desde fuentes desconocidas; con base en lo anterior, se deben instalar aplicaciones únicamente autorizados por ComWare.

2.1.21.1.4. Los colaboradores de ComWare deben, cada vez que el sistema de sus dispositivos móviles notifique una actualización disponible, aceptar y aplicar la nueva versión.

2.1.21.1.5. Los colaboradores deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles.

2.1.21.1.6. Bajo su responsabilidad y riesgo es permitido a los usuarios de Comware el almacenamiento de videos, fotografías o información personal en los dispositivos móviles corporativos asignados. En caso de pérdida, la compañía no es responsable de la recuperación asociada con dicha información.

2.1.21.1.7. Los colaboradores de Comware deben informar al Service Desk en caso de observar comportamientos anómalos asociados con las funcionalidades de los dispositivos.

2.1.21.1.8. No se debe alojar localmente información clasificada como secreta y altamente secreta dentro de los dispositivos móviles, pertenecientes a ComWare.

2.1.21.1.9. Los Colaboradores de ComWare deben evitar deshabilitar el GPS de los dispositivos móviles.

2.1.21.1.10. Los Colaboradores no deben instalar en dispositivos móviles (Celulares Inteligentes y Tabletas entre otros), plataforma de almacenamiento en la nube corporativa.

2.1.21.1.11. Los Colaboradores deben abstenerse de usar memoras externas, ni almacenar información corporativa en dispositivos móviles (Celulares Inteligentes y Tabletas entre otros), plataforma de almacenamiento en la nube corporativa.

2.1.21.2. De la Organización:

2.1.21.2.1. La Gerencia de Sistemas de Información desarrollará las políticas para el uso seguro de los dispositivos móviles corporativos mecanismos de protección de los dispositivos móviles corporativos que hagan uso de los servicios provistos por ComWare.

2.1.21.2.2. La Gerencia de Infraestructura y Data Center, junto con la Gerencia de Soluciones de Seguridad, deberán establecer las configuraciones aceptables para los dispositivos móviles corporativos o personales que hagan uso de los servicios provistos ComWare.

2.1.21.2.3. La Gerencia de Infraestructura y Datacenter o Sistemas de Información con autorización del usuario, configurará la opción de borrado remoto de información y activar la opción de cifrado de memoria de los dispositivos móviles corporativos (Celulares Inteligentes, Tabletas entre otros), con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

2.1.21.2.4. La gerencia de Infraestructura y Data Center o Sistemas de Información, debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz), para los dispositivos móviles que serán entregados a los colaboradores. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

2.1.21.2.5. En caso de pérdida o hurto el usuario debe reportar a Service Desk, para que la información sea borrada

2.1.21.2.6. En usos de sus facultades administrativas, y por solicitud de Gestión Humana, Comware es autónomo para borrar toda la información.

2.1.21.2.7. La Gerencia de infraestructura y Data Center, y la Gerencia de Soluciones de Seguridad determinarán el software de protección que se deberá instalar en los dispositivos móviles corporativos.

2.1.21.2.8. La Gerencia Sistemas de Información y la Gerencia de Soluciones de Seguridad determinarán los aplicativos que se restringirán, durante el periodo laboral y el entorno geográfico asociado.

2.1.21.2.9. Para fines laborales, Comware tiene la autonomía para verificar la ubicación de los dispositivos que pertenecen a la Compañía, a través de la herramienta asociada con la gestión de movilidad.

2.1.22. Políticas de Uso de Token y Firmas Digitales

2.1.22.1. Cada área que usa token de seguridad debe asignar un colaborador Administrador de los mismos con la potestad para autorizar las solicitudes de acceso de acuerdo con lo debido por el dueño.

2.1.22.2. Los Administradores de los token de seguridad deben procesar las solicitudes de dichos token según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria.

2.1.22.3. Los Administradores de los token deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.

2.1.22.4. Los Administradores de los token deben entregar a los Colaboradores designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta para custodia de los mismos.

2.1.22.5. Los Administradores de los token deben dar avisos a las entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.

2.1.22.6. Los Administradores de los token deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

2.1.22.7. Los usuarios deben devolver el token asignado en estado operativo al Administrador de los token cuando el vínculo laboral con el Comware, se dé por terminado o haya cambio de cargo, para obtener el paz y salvo, el cual será requerido para legalizar la finalización del vínculo laboral con la Compañía.

2.1.22.8. El almacenamiento de los token debe efectuarse bajo estrictas medidas de seguridad, sobre asignado para cada token, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de personal no autorizado.

2.1.22.9. Los usuarios deben notificar al Administrador de los token en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos token.

2.1.22.10. Los usuarios no deben permitir que terceras personas observen la clave que genera el token, así como no deben aceptar ayuda de terceros para la utilización del token.

2.1.22.11. Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como colaboradores de COMWARE, En caso de que suceda algún evento irregular con los token los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

2.1.22.12. Los usuarios deben mantener los token asignados en un lugar seco y no introducirlos en agua u otros líquidos.

2.1.22.13. Los usuarios deben evitar exponer los token a campos magnéticos y a temperaturas extremas.

2.1.22.14. Los usuarios deben evitar que los token sean golpeados o sometidos a esfuerzo físico.

2.1.22.15. Los usuarios no deben usar los token fuera de las instalaciones del Comware para evitar pérdida o robo de estos.

2.1.23. Política de Escritorio y Pantalla Limpia

Es responsabilidad de los colaboradores seguir las buenas prácticas y lineamientos:

2.1.23.1. Portar el Carné en un lugar visible al momento de ingresar a las instalaciones físicas de ComWare S.A.

2.1.23.2. Bloquear manualmente la sesión del computador, al momento de ausentarse del puesto de trabajo.

2.1.23.3. Asegurar la información física, clasificada como confidencial, secreto o dato personal, en lugares seguros como cajonera de puesto de trabajo o archivo de gestión del proceso.

2.1.23.4. Evitar exponer información confidencial en lugares públicos, como salas de reuniones y asegurar el borrado la información expuesta en los tableros.

2.1.23.5. Asegurar los dispositivos móviles en un lugar seguro bajo llave, cuando se ausente por largos periodos de tiempo del puesto de trabajo.

2.1.23.6. Asegurar mantener el escritorio del PC asignado sin archivos.

2.1.23.7. Asegurar la información digital, clasificada como confidencial, secreto o dato personal en la plataforma de almacenamiento corporativo y restringir el acceso solo a las personas autorizadas.

2.1.23.8. Asegurar los documentos personales de identificación en un lugar seguro.

2.1.23.9. Asegurar la no utilización de hojas reutilizables con información confidencial o dato personal como: (HV, Información, Financiera, Certificaciones laborales, Arquitectura, Ofertas comerciales, dato personal etc.)

2.1.23.10. Reportar dispositivos de almacenamiento externos USB olvidados en las instalaciones y asegurar no conectarla en los equipos de cómputos corporativos.

2.1.23.11. Seguir los lineamientos para la disposición final de información clasificada como confidencial y secreto

2.1.23.12. Asegurar la confidencialidad de las contraseñas y el cambio de estas.

2.1.24. Política de cifrado

Es responsabilidad del Comité de Seguridad de la Información definir qué información debe ser protegida a través de mecanismos definidos para tal fin.

Es responsabilidad de la Gerencia de Infraestructura implementar los mecanismos de cifrado para la protección de la información que se almacena y transfiere a través de correo electrónico.

Los colaboradores que manejan y transfieran información secreta deben utilizar mecanismos establecidos para proteger la información a través de correos electrónicos.

2.2. Procedimientos que Apoyan la Política de Seguridad.

2.2.1. Todos los procedimientos que soportan la presente política, deben estar alineados con los estándares NTC ISO27001, NTC ISO 9001 y cuando aplique, ITIL 2011.
2.2.2. Todos los procedimientos que soportan la presente política deben estar incorporados dentro del Sistema de Gestión de la Calidad de ComWare S.A. y cumplir con los lineamientos establecidos por este Sistema.

2.3. Gestión de los Incidentes de la Seguridad de la Información.

2.3.1. Para la Gestión de Incidentes de Seguridad de la Información, se deberá seguir el procedimiento que se tiene establecido dentro del Modelo de Gestión del Servicio de TI establecido para el proceso de Gestión de TIC´s y que incluye las actividades desarrolladas por las Gerencias de Sistemas de Información e Infraestructura.

2.4. Proceso Disciplinario.

2.4.1. Se realizará el proceso disciplinario formal para los colaboradores que hayan cometido alguna violación de la presente Política de Seguridad de la Información.

2.4.2. El proceso disciplinario también se constituye como un elemento de disuasión para evitar que los colaboradores, contratistas y demás personal de la Compañía viole las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de Gestión humana de la Gerencia del mismo nombre.

2.5. Gestión de la Continuidad del Negocio.

2.5.1. Es el conjunto de políticas, procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la Empresa, para proteger sus procesos críticos contra fallas mayores en los sistemas de información y/o en la infraestructura tecnológica crítica.
2.5.2. Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI de ComWare S.A. podrán ser restaurados dentro de escalas de tiempo razonables**.**
2.5.3. La Compañía deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:
2.5.4. Identificación y asignación de prioridades a los procesos críticos de TI de la Compañía de acuerdo con su impacto en el cumplimiento de la misión de la Empresa.
2.5.5. Documentación de la estrategia de continuidad del negocio.
2.5.6. Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
2.5.7. Plan de pruebas de la estrategia de continuidad del negocio.

2.5.8. La continuidad del negocio deberá ser gestionada por la Gerencia de Infraestructura de la Compañía.
2.5.9. La alta dirección de la Compañía será la responsable de velar por la implantación de las medidas relativas a ésta.
2.5.10. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.
2.5.11. La alta dirección de la Compañía, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

2.6. Cumplimiento

2.6.1. Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los colaboradores, contratistas y demás personal de la Compañía. En caso de que se violen las políticas de seguridad, ya sea de forma intencional o por negligencia, la Compañía tomará las acciones disciplinarias y legales correspondientes**.**

2.6.2. Las Políticas Corporativas de Seguridad de la Información deben prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

2.7. Controles.

2.7.1. Las Políticas Corporativas de Seguridad de la Información están soportadas por un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este documento. Los usuarios de los servicios y recursos de tecnología de la Compañía pueden consultar los procedimientos a en la herramienta de gestión documental Docmager.

2.8. Declaración de Aplicabilidad.

2.8.1. La Declaración de Aplicabilidad (Statement of Applicability -SOA) referenciado en la numeral 6.2 de la NTC ISO-IEC 27001 es un documento que lista los objetivos y controles que se van a implementar en la Compañía, así como las justificaciones de aquellos controles que no van a ser implementados.

2.8.2. Para el caso específico de la Compañía, este tipo de análisis se hace evaluando el cumplimiento de la norma NTC ISO-IEC 27002, para cada uno de los controles establecidos en los 14 dominios o temas relacionados con la gestión de la seguridad de la información que esta norma específica; y una vez se complete este análisis ya se puede realizar la Declaración de Aplicabilidad.