ÍNDICE

INTRODUCCION

La información es un recurso que, como el resto de los activos, tiene valor para la organización y por consiguiente debe ser debidamente protegida. Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de Distribuidora Cummins Perú S.A.C. (DCP).

1. OBJETIVO

El objetivo del establecimiento del Reglamento Interno de Seguridad de la Información es el de asegurar que la confiabilidad, disponibilidad, confidencialidad e integridad de cada objeto de información del cual Distribuidora Cummins Perú S.A.C. (DCP) sean propietarios o que se encuentre confiada a éstos, estén protegidos de una manera consistente con el valor atribuido a cada objeto por DCP según las mejores prácticas de administración de manejos de riesgo.

2. ALCANCE

El presente reglamento aplica para todos los funcionarios, empleados, contratistas y practicantes de DCP así como a demás personas relacionadas con terceras partes que utilicen la plataforma tecnológica y los servicios tecnológicos de DCP.

3. RESPONSABILIDAD

El **Gerente de TI** es responsable de asegurar el cumplimiento, difusión y actualización del presente reglamento.

4. DOCUMENTOS DE REFERENCIA

No Aplica.

5. DEFINICIONES

5.1. **Reglamento:** son instrucciones mandatarios que indican la intención de la alta gerencia respecto a la operación de la organización.

5.2. **Recurso Informático:** Elementos informáticos (base de datos, sistemas operativos, redes, sistemas de información y comunicaciones) que facilitan los servicios informáticos.

5.3. **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

5.4. **Usuarios Terceros:** Todas aquellas personas, naturales o jurídicas, que no son funcionarios de DCP, pero que por las actividades que realizan en la organización, deben tener acceso a recursos informáticos.

5.5. **Brecha de Seguridad:** Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma.

5.6. **Confidencialidad:** Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

5.7. **Integridad:** Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

5.8. **Disponibilidad:** Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

5.9. **Confiabilidad:** La información generada es adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

5.10. **Dueño de la Información:** Son los funcionarios, empleados, unidades de negocio o áreas responsables de la generación o recopilación de la información, con competencia para administrar y disponer de su contenido.

6. DIAGRAMA DE FLUJO

No Aplica.

7. DESARROLLO

7.1. Sobre el Acceso a la Información

7.1.1. Todos los funcionarios, empleados, contratistas y practicantes que trabajan para DCP deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a DCP, se debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación, constando éste en el contrato o acuerdo de servicios.

7.1.2. Para que un funcionario, empleado, contratista o practicante tenga acceso a los servicios y recursos tecnológicos dispuestos por DCP se requiere que el jefe inmediato, sub-gerencia o gerencia de la unidad de negocios relacionada, solicitar a Tecnología de la Información mediante solicitud escrita, la activación de dichos servicios con el perfil requerido y las restricciones de algunos servicios.

7.1.3. Cada vez que se recibe una computadora de escritorio o portátil para darle accesos a servicios tecnológicos que brinda DCP a los usuarios, Tecnología de la Información es responsable y está obligada de entregar el equipo con todos los servicios instalados, configurados y en operación. Esto es, verificación y última verificación de parches de seguridad del sistema operativo, instalación y configuración del antivirus, herramientas de ofimática y cualquier otra cuyo perfil de usuario justifique su instalación.

7.1.4. El otorgamiento de acceso a la información y los sistemas de información está regulado mediante las políticas específicas, normas y procedimientos definidos para tal fin.

7.1.5. Todos los privilegios para el uso de los recursos informáticos, servicios informáticos y sistemas de información de DCP, deben terminar inmediatamente después de que el funcionario, empleado o practicante deja de prestar sus servicios a la compañía.

7.1.6. Contratistas, proveedores o terceras personas solamente tendrán privilegios durante el periodo de tiempo requerido y autorizado para llevar a cabo las funciones aprobadas. En estos casos deberán firmar, como parte de su contrato, una cláusula de obligación de cumplimiento del Reglamento Interno de Seguridad de la Información y de todas aquellas políticas, normas y procedimientos sobre esta materia.

7.1.7. Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la compañía, la cual debe realizarse de acuerdo a la importancia de la información en la operación normal de la compañía.

7.1.8. Mediante el registro de eventos en los diferentes recursos informáticos de la plataforma tecnológica se realizará un seguimiento a los accesos realizados por los usuarios a la información de la

compañía, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, confiabilidad, confidencialidad y disponibilidad de la información se deberán documentar y realizar las acciones pertinentes para su solución.

7.2. Sobre la Gestión de Cambios en los Sistemas de Información

7.2.1. Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios dueños y responsables de la información y del proceso y aprobado por los funcionarios de Tecnología de la Información, con el visto bueno y supervisión del jefe inmediato.

7.2.2. Los responsables de la administración de accesos de Tecnología de la Información tendrán la facultad de rechazar la solicitud de cambios si esta pone en riesgo la integridad, confiabilidad, confidencialidad y disponibilidad de la información.

7.2.3. Bajo ninguna circunstancia un cambio puede ser requerido, aprobado e implementado por la misma persona.

7.2.4. Para la administración de los cambios se efectuará el procedimiento correspondiente de control de cambios definidos por DCP, de acuerdo con el tipo de cambio definido por la plataforma tecnológica.

7.2.5. Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implementación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos para el adecuado control de calidad.

7.2.6. Todo cambio en un recurso informático de la plataforma tecnológica relacionado con la modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no ponga en riesgo la seguridad existente.

7.3. Sobre Seguridad de la Información

7.3.1. Los funcionarios, empleados, contratistas y practicantes de DCP son responsables de la información que manejan y deberán cumplir los lineamientos generales y específicos dados por la compañía y por la Ley, para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

7.3.2. Los funcionarios, empleados, contratistas y practicantes de DCP no deben suministrar alguna información de la compañía a ningún ente externo, ni los controles de los sistemas informáticos en uso, ni la forma en que son implantados sin la autorización de Tecnología de la Información

7.3.3. Los funcionarios, empleados, contratistas y practicantes de DCP que tienen asignados equipos portátiles deben mantenerlos asegurarlos con candados, alarmas u algún otro medio de seguridad dentro de las instalaciones de DCP o en áreas accesibles al público como los aeropuertos, hoteles, el auto, centros de conferencias, universidades, bibliotecas y hospitales.

7.3.4. Los funcionarios, empleados, contratistas y practicantes de DCP no deben dejar sus estaciones de trabajo, computadoras personales o terminales desatendidas, sin antes, salir y bloquear el sistema.

7.3.5. Todo funcionario, empleado, contratista y practicante que utilice la plataforma tecnológica y los servicios tecnológicos disponibles tienen la responsabilidad de velar por la integridad, confiabilidad, confidencialidad y disponibilidad de la información que maneje, especialmente si dicha información ha sido identificada como confidencial o restringida.

7.3.6. Después de que un funcionario, empleado, contratista y practicante deja de prestar sus servicios a DCP, éste se compromete e entregar toda la información respectiva de su trabajo realizado al jefe inmediato. Una vez retirado el funcionario, empleado, contratista y practicante debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la compañía, directamente o a través de terceros.

7.3.7. La propiedad intelectual desarrollada o concebida mientras el funcionario, empleado, contratista y practicante se encuentre en sitios de trabajo de la compañía, es de propiedad exclusiva de DCP. Esta política incluye patentes, derechos de reproducción, marca registrada, planes, estrategias, productos, investigaciones pagadas por la compañía, estudios ambientales y de otros propósitos, programas de computación, códigos fuentes, documentación, otros derechos de propiedad intelectual y otros materiales.

7.3.8. Todas las estaciones de trabajo deben apagarse al finalizar el horario de trabajo, con excepción de los servidores y estaciones de trabajo independientes que estén ubicados en áreas con controles estrictos de acceso físico y de suministro eléctrico.

7.3.9. Los funcionarios, empleados, contratistas y practicantes que detecten el mal uso de la información están en la obligación de reportar el hecho al área de Seguridad de Información.

7.3.10. Todo funcionario, empleado, contratista y practicante que maneje información clasificada como restringida y confidencial deberá de colocar una contraseña de protección del documento contra aperturas no autorizadas según la disponibilidad de la herramienta ofimática.

7.3.11. La persona a la cual se le comparte un documento el cual haya sido protegido con contraseña, queda totalmente prohibido de deshabilitarla o manipularla.

7.3.12. La persona a la cual se le comparte un documento el cual haya sido protegido con contraseña, queda totalmente prohibido de compartirlo y divulgarla sin la previa autorización del dueño del documento compartido.

7.3.13. Los equipos de cómputo móviles asignados a usuarios serán encriptados obligatoriamente.

7.4. Sobre el Uso del Correo Electrónico e Internet

7.4.1. El sistema de correo electrónico e Internet prestados por DCP deben ser utilizados únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de contratistas y practicantes.

7.4.2. La compañía se reserva el derecho a acceder y develar los mensajes enviados por medio del sistema de correo electrónico cuando esta represente un riesgo contra la confiabilidad, disponibilidad, confidencialidad e integridad de la información, la compañía para dicho fin establecerá procedimientos respectivos para garantizar el cumplimiento de la normativa vigente en materia de privacidad de datos personales.

7.4.3. Los funcionarios, empleados, contratistas y practicantes que hayan recibido aprobación hacer uso de una cuenta de correo electrónico y para tener acceso a internet a través de las estaciones de trabajo de la compañía o computadoras portátiles personales, deberán aceptar, respetar y aplicar las políticas, procedimientos y normas aprobadas para su uso.

7.4.4. DCP permite el acceso a internet en equipos de la plataforma de la compañía a través de otras empresas prestadoras de servicio de internet haciendo uso de dispositivos inalámbricos diferentes al servicio disponible propio. Los usuarios deberán contar con una autorización y serán registrados en Tecnología de la Información con el fin de minimizar los riesgos a la integridad de la información y la seguridad de los sistemas de información de la compañía.

7.4.5. El personal temporal subcontratado para suplir funciones de empleados o funcionarios de DCP y podrán contar con una cuenta de correo la cual deberá de mostrar como nombre de dirección, la empresa intermediadora del servicio, no debiendo ser esta cuenta nominal.

7.5. Sobre la Seguridad en los Sistemas de Información

7.5.1. El acceso a los servicios y sistemas de información de DCP es un privilegio y no un derecho.

7.5.2. Todos los sistemas de información deben de cumplir con lo siguiente:

- Administración de Usuarios: Establecen como deben ser utilizadas las claves de ingreso a los sistemas de información. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los periodos de vigencia de la misma, entre otros.
- Rol de Usuario: Los sistemas operativos, bases de datos y aplicativos deben contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el de la Administración de Usuarios.
- Bitácora de Operaciones: Hace referencia a los registros de los sucesos y transacciones relativos a la operación.

7.5.3. El control de acceso a los sistemas de información de la compañía debe realizarse por medio de códigos de identificación y claves de acceso únicas para cada usuario los cuales determinan la cuenta que los identifica como individuos específicos.

7.5.4. La configuración de las claves de acceso a los sistemas de información será realizada por los propios usuarios salvo casos en que la funcionalidad del servicio impida esta asignación. Las claves de acceso a los sistemas de información que designen los funcionarios, empleados, contratistas y practicantes son responsabilidad de cada uno de ellos y no deben ser divulgados a ninguna persona.

7.5.5. El uso de cuentas comunes o grupales está permitido siempre y cuando esté plenamente justificada y autorizada. Para este caso se debe tener un registro de los funcionarios, empleados, contratistas y practicantes con acceso a este tipo de cuentas.

7.5.6. Los usuarios son responsables de todas las actividades llevadas a cabo con su cuenta de identificación de usuario y sus claves personales.

7.5.7. Todo sistema de información debe tener definido los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

7.5.8. Antes que un nuevo sistema de información se desarrolle o adquiera, los miembros ejecutivos del área que lo requieren en conjunto con Tecnología de la Información, deberán definir las especificaciones y requerimientos de seguridad necesarios.

7.5.9. La asignación de roles y perfiles a los usuarios deberá de ser aprobadas por distintos niveles de dueños y responsables de la información dependiendo del nivel de criticidad de la información y funcionalidades a las cuales tendrá acceso. Esta aprobación se deberá hacer luego de la sustentación de la necesidad por parte de la Gerencia solicitante y la descripción del puesto del usuario por parte de RRHH.

7.5.10. Toda la información del servidor de Base de Datos que sea restringida, confidencial o valiosa debe tener controles de acceso y sometida a procesos de respaldo para garantizar que no sea inapropiadamente modificada, borrada o no recuperable.

7.5.11. El personal temporal subcontratado para suplir funciones de empleados o funcionarios de DCP podrán contar con una cuenta propia nominal para el ingreso a los sistemas de la empresa previa autorización, estando prohibido la asignación y el uso de la(s) cuenta(s) del empleado al cual reemplazan.

7.6. Sobre la Seguridad en Redes de Comunicación

7.6.1. Las direcciones internas, topología, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la compañía, deberán ser consideradas y tratadas como información confidencial.

7.6.2. Todos los relojes de todos los sistemas de procesamiento de información y de las computadoras multiusuario conectados a la red interna de DCP deben tener siempre la hora actual reflejada en sus relojes internos en base a una fuente acordada y exacta de tiempo, con el fin, de tener registros confiables de los eventos, actualizaciones automáticas de software, duplicación de bases de datos, cambios automáticos de claves y otras actividades relacionadas con la seguridad.

7.6.3. La red WAN debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso. Cada una de las sedes deberá de mantener los lineamientos de seguridad implementados en este documento de política de seguridad de la información.

7.6.4. Todas las conexiones desde redes externas en tiempo real que accedan a la red interna de la compañía, debe pasar a través de los sistemas de protección electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

7.6.5. Todo intercambio electrónico de información o interacción de sistemas electrónicos de información con entidades externas deberá estar soportado con un acuerdo de formalización.

7.6.6. Los equipos de DCP que se conecten directamente con computadoras de entidades externas, deberán hacer uso de conexiones seguras, previa autorización de Tecnología de la Información.

7.6.7. Está prohibido la conexión de equipos de red como swtiches o routers diferentes a aquellos que Tecnología de la Información instala dentro de cualquier local, oficina o ambiente de DCP.

7.7. Sobre la Seguridad para Terceros

7.7.1. Los dueños de recursos tecnológicos e informáticos que no sean propiedad de DCP y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente deben recibir y aceptar el documento de políticas de seguridad.

7.7.2. Cuando se requiera utilizar recursos tecnológicos u otros elementos de propiedad de DCP para el funcionamiento de recursos que no sean propios de la compañía y que deban utilizarse en sus instalaciones, los recursos serán administrados por Tecnología de la Información.

7.7.3. Los usuarios terceros tendrán acceso a los servicios y recursos tecnológicos de DCP que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser solicitados por quien será el jefe superior o coordinar y aprobados por el área de Seguridad de Información. En todo caso deberán firmar una solicitud de activación y acceso a servicios tecnológicos y aceptarán a dar un buen uso de los recursos y servicios.

7.7.4. Si se requiere un equipo con conexión inalámbrica no auditable, este equipo no podrá en ningún momento estar conectado a la red de DCP al mismo tiempo.

7.7.5. La conexión entre sistemas internos de la compañía y otros de terceros debe ser aprobada y certificada por Tecnología de la Información con el fin de no comprometer la seguridad de la información interna de la compañía.

7.7.6. Los equipos de usuarios, proveedores o terceros que requieran estar conectados a la red interna de DCP, deben aceptar como condición ser revisados por Tecnología de la Información con el fin de asegurar que sus sistemas cumplan con todas las normas de seguridad informática vigentes en la compañía.

7.7.7. Como requisito para interconectar la red de DCP con la de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por DCP. La entidad se reserva el derecho de monitorear y auditar estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La compañía se reserva el derecho de cancelar y terminar inmediatamente las conexiones a sistemas de terceros que no cumplan con los requerimientos internos establecidos por DCP.

7.8. Sobre el Software Utilizado

7.8.1. Todo software que utilice DCP será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de compra la compañía o reglamentos internos.

7.8.2. Debe existir una cultura tecnológica al interior de DCP que garantice el conocimiento por parte de los funcionarios, empleados, contratistas y practicantes de las implicancias que tiene el instalar software ilegal en las computadoras de DCP.

7.8.3. Existirá un inventario de las licencias de software de DCP que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

7.8.4. El software instalado en un computador deberá de ser aquel que el perfil del usuario requiera.

7.8.5. Las instalaciones o cambios en la configuración de software en los computadores de los usuarios sólo podrán ser realizadas por Tecnología de la Información o con autorización de ésta. Tecnología de la Información podrá en todo momento desinstalar cualquier software el cual no haya sido autorizado sin responsabilizarse por el prejuicio que éste pueda causar al usuario.

7.8.6. La naturaleza de software gratuito, de prueba o freeware no la exime de ser susceptible a los controles del párrafo anterior.

7.8.7. Tecnología de la Información es la responsable de realizar revisiones periódicas para asegurar que sólo programas autorizados estén instalados en las computadoras de la compañía.

7.8.8. El antivirus y su agente remoto deben instalarse en todas las estaciones de trabajo y servidores en DCP con la configuración definida por Tecnología de la Información y/o recomendada por el proveedor, las mínimas opciones configuradas deben contemplar la revisión automática de los medios de computación removibles, actualizaciones automáticas y revisiones diarias de análisis rápido a una hora apropiada. Las excepciones deben documentarse con el fin de guardar pistas de auditoría.

7.8.9. Los funcionarios, empleados, contratistas y practicantes de DCP no deben ingresar en procesos de Internet que involucren el uso de código móvil (Javascript, VBScript, Java Applets, controles de ActiveX, Animaciones, Macros, Plugins, entre otros), y permitir la ejecución o colocación del código móvil en sus máquinas.

7.8.10. Todo módulo o utilidad del sistema operativo que no ha de utilizarse, y que no sea necesario para el funcionamiento de otro software esencial del sistema, debe ser eliminado o desactivado de las estaciones de trabajo del personal de DCP, esto debe ser evaluado y ejecutado por Tecnología de la Información.

7.9. Sobre el Mantenimiento y Actualización de los Equipos de Cómputo

7.9.1. Tecnología de la Información debe crear, mantener y ejecutar un programa de mantenimiento preventivo y correctivo de los servidores críticos para asegurar su continua disponibilidad y continuidad, debiendo considerar los siguientes aspectos:

- El programa para los servidores críticos debería considerar como mínimo 2 mantenimientos al año o de acuerdo con los intervalos y especificaciones recomendadas por el proveedor.

- Deben implementarse los controles apropiados si el mantenimiento de los servidores críticos es realizado por personal externo (outsourcing); donde sea necesario, la información sensible debería eliminarse del equipo.

- Deben guardarse los registros de todas las fallas sospechosas o reales y de todo el mantenimiento preventivo y correctivo.

7.9.2. Tecnología de la Información es la encargada de la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar.

7.9.3. Está estrictamente prohibido dar mantenimiento a equipos de cómputo que no sean de propiedad de DCP.

7.9.4. Cualquier cambio que se requiera realizar en los equipos de cómputo de DCP (cambio de procesador, aumento de memoria, aumento de capacidad de disco duro, etc.), debe realizarlo exclusivamente personal de Tecnología de la Información o terceros bajo supervisión y autorización de ésta.

7.9.5. La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por personal de Tecnología de la Información o terceros bajo supervisión y autorización de ésta.

7.9.6. Los equipos tecnológicos instalados en la plataforma tecnológica (PC, routers, switches, antenas, accesspoints, etc.) no deben moverse o reubicarse sin el conocimiento y aprobación previa de Tecnología de la Información. No se incluye en este control los computadores portátiles.

7.10. Sobre el Almacenamiento y Respaldo de la Información

7.10.1. La información que es soportada por la infraestructura de tecnología informática de DCP, deberá de ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

7.10.2. Debe existir una definición formal de la estrategia de generación, almacenamiento, retención y rotación de las copias de respaldo.

7.10.3. El almacenamiento de la información deberá de realizarse interna o externamente a DCP, esto de acuerdo con la importancia de la información para la operación.

7.10.4. Los funcionarios, empleados, contratistas y practicantes de una sede o segmento de la WAN fuera del ámbito operativo de Tecnología de la Información y que sea dueña de información, serán los

responsables de respaldar la información producida por ésta, siguiendo el procedimiento definido por Tecnología de la Información para proteger la información de los usuarios.

7.10.5. Los funcionarios y empleados son responsables de los respaldos de información en sus computadoras, siguiendo las indicaciones técnicas dadas por Tecnología de la Información.

7.11. Sobre la Seguridad Física y Ambiental

7.11.1. DCP deberá contar con mecanismos de control de acceso tales como tarjetas inteligentes y sistemas de alarmas en los ambientes que la compañía considere críticas además de tener rótulos que indiquen su condición de áreas restringidas. Estás áreas deberán contar con elementos de control de incendio, inundación y alarmas.

7.11.2. Los visitantes a estos ambientes deberán de ser escoltados durante todo el tiempo por un empleado autorizado, asesor o contratista. Esto significa que se requiere una escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta, incluyendo clientes, antiguos empleados o miembros de la familia del trabajador.

7.11.3. Siempre que un trabajador se dé cuenta que un visitante no escoltado se encuentra dentro de áreas restringida de la compañía, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en el área restringida e informar a los responsables de la seguridad del edificio.

7.11.4. El Centro de Procesamiento de Datos, el área de Tecnología de la Información y otras áreas que la compañía considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

7.11.5. Los gabinetes de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

7.11.6. Los particulares en general, entre ellos, los familiares de los funcionarios y empleados, no están autorizados para utilizar los servicios y recursos tecnológicos de DCP.

7.11.7. Las computadoras personales y estaciones de trabajo críticas en DCP deben estar equipadas con sistemas que suministren corriente eléctrica sin interrupciones (UPS o grupos electrógenos), filtros de potencia eléctrica o supresores de alzas de voltaje aprobados por Tecnología de la Información

7.11.8. La instalación y el mantenimiento de los cables de electricidad y de telecomunicaciones deben ejecutarse e implementarse considerando las mejores prácticas y las normas establecidas de seguridad de la industria con el fin de evitar cualquier intercepción no autorizada de la transmisión de datos o daños al sistema.

7.11.9. El equipo informático, información o software no deben ser sacados fuera de las instalaciones de DCP sin autorización previa.

Se deben considerar las siguientes pautas:

- El equipo, información o software no deben ser sacados fuera del local de trabajo sin autorización de su respectiva Gerencia y de Tecnología de la Información; las Gerencias tendrá conocimiento y autorizarán la salida de cualquier equipo a ser trasladado fuera de las instalaciones de DCP. Las Gerencias deben determinar la necesidad de que el equipo sea trasladado y garantizar que se sigan las medidas apropiadas de seguridad mientras el equipo esté fuera de las instalaciones de DCP.

- Los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de equipos o software deben estar claramente identificados y autorizados mediante un documento formal (aprobado y firmado)

- La salida y el retorno de los equipos informáticos o software deben ser verificados a la entrada y a la salida del local de trabajo por los responsables de la seguridad del edificio con el fin de asegurar la conformidad.

7.12. Sobre la Política de Pantalla y Escritorios Limpios

7.12.1. Si no ha habido actividad en un terminal, estación de trabajo o computador personal por 10 minutos, el sistema automáticamente debe invocar un protector de pantalla corporativo protegido con contraseña, suspender la sesión y solicitar una contraseña para restablecer la sesión.

7.12.2. Fuera del horario normal de trabajo, todos los funcionarios, empleados, contratistas y practicantes de DCP deben dejar limpios sus escritorios y áreas de trabajo, de papeles y medios de almacenamiento removibles (CDs, USBs, discos externos, memorias, etc.) con el fin de evitar que personas que estén en el edificio fuera del horario de trabajo, tengan acceso a información sensible, esta política también incluye máquinas de fax desatendidas, impresoras, pizarrones en salones de conferencia y otros lugares donde la información sensible pudiera estar al descubierto.

7.13. Sobre los Procedimientos de Contingencia

La Presidencia Ejecutiva de DCP o a quien delegue, debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, incendio, terrorismo, inundación, etc.

7.14. Sobre la Administración de la Seguridad de la Información

7.14.1. Cualquier brecha de seguridad o sospecha en la mala utilización de internet, la red corporativa o intranet, los servicios y recursos tecnológicos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial a Tecnología de la Información.

7.14.2. Las empresas contratistas que realicen la administración de servicios tecnológicos son responsables por la implementación, permanencia y administración de los controles sobre los recursos computacionales. La implementación debe ser consistente con las prácticas establecidas o aceptadas por DCP.

7.14.3. Tecnología de la Información divulgará, las políticas, normas y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará a Control Interno, los casos de incumplimiento con copia a RRHH y SSOMAC.

7.15. Sobre la Administración de los Equipos de Cómputo

7.15.1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores y equipo accesorios), que esté o sea conectado a la red de DCP, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a las normas y procedimientos de instalación que emite Tecnología de la Información.

7.15.2. Tecnología de la Información en coordinación con el área de Contabilidad e Impuestos (activo fijo) deberá tener un registro de todos los equipos propiedad de DCP.

7.15.3. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

7.15.4. El equipo de la compañía que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica, su acceso que Tecnología de la Información tiene establecido en su normatividad de este tipo.

7.15.5. La protección física de los equipos es de responsabilidad de los funcionarios, empleados, contratistas o practicantes a los cuales se les asigna, y corresponde notificar los movimientos en caso de que existan, a las áreas correspondientes (Tecnología de la Información, Contabilidad e Impuestos-activo fijo, y otros de competencia).

7.15.6. No está permitida la conexión a la red de DCP ni el uso de los recursos y servicios tecnológicos de equipos personales de funcionarios, empleados, contratistas y practicantes.

7.16. Sobre la Seguridad y la Gestión de los Medios Removibles

7.16.1. Todos los medios de computación removibles utilizados en DCP deben ser autorizados, formateados y emitidos únicamente por el área de Tecnología de la Información (no deben ser de uso personal), los medios que contengan información de DCP deberán contar con un proceso de cifrado, de esta manera, estos medios serán ilegibles en computadoras externas a la organización.

7.16.2. Como regla general, los puertos USB de los computadores entregados al personal serán desactivados para su uso como dispositivo de almacenamiento. La activación deberá de ser solicitada y aprobada por la gerencia de B.U. solicitante y con el V°B° del área de Seguridad de Información. La activación podrá ser permanente o temporal según la solicitud.

7.16.3. La información de la Compañía solo debe ser almacenada en equipos y sistemas informáticos de propiedad de esta. Los colaboradores, proveedores y demás terceros no deberán almacenar ni efectuar tratamiento alguno de información en dispositivos no autorizados o ajenos a la propiedad de la Compañía, estando además prohibido almacenar información de índole íntima personal en dispositivos de almacenamiento removible de la Compañía.

7.16.4. Los colaboradores que cuenten con dispositivos de almacenamiento externo proporcionados por la Compañía, no deberán efectuar ni intentar hacer cambios a la configuración de seguridad de dichos dispositivos tales como desactivar el sistema de encriptación, entre otros.

7.16.5. Todos los medios de almacenamiento de información portátiles (CDs, USBs, discos externos, memorias, etc.) que contengan información de la Compañía, deben estar físicamente guardados en lugares seguros y con llave cuando no estén en uso o fuera del horario normal de trabajo.

7.16.6. Los colaboradores serán responsables de la debida custodia de los dispositivos asignados, debiendo garantizar su uso diligente, no exponiéndolo a riesgos de pérdida o robo. En caso esto ocurriese, deberá reportar dicho evento inmediatamente al área de Tecnología de la Información, los costos de reposición serán a cargo de cada BU solicitante.

7.16.7. Los dispositivos de almacenamiento removible deberán ser devueltos cuando estos presenten algún desperfecto, cuando no sea necesario utilizarlos, cuando el colaborador responsable cese en su relación laboral o cuando el proveedor tercero culmine la prestación de sus servicios, dicha devolución deberá ser efectuada al área de Tecnología de la Información.

7.16.8. Cuando la información de la Compañía se borra de un disco, cinta u otro medio reutilizable de almacenamiento de datos, se debe acompañar dicha acción con una operación repetida de re-

escritura para eliminar de forma segura la información, para ello, Tecnología de la Información debe utilizar un procedimiento autorizado para este proceso.

7.16.9. La destrucción de la información resguardada en medios informáticos de almacenamiento, debe llevarse a cabo sólo con métodos de destrucción autorizados por Tecnología de la Información, entre ellos tenemos: la desmagnetización, destrucción física, programas de re-escritura u otro método que inutilice los medios de almacenamiento.

7.16.10. Si la destrucción de información es realizada por personal de una empresa externa se debe verificar los antecedentes y reputación de la empresa, firmar acuerdos de confidencialidad y solicitar un certificado de destrucción.

8. DOCUMENTOS, REGISTROS Y CONTROLES ASOCIADOS

No Aplica.

9. ANEXOS

No Aplica.

10. CONTROL DE CAMBIOS

Versión	Fecha	Sección/Ítem	Cambio realizado
01	14/10/2020	7.3.5	Se adecua punto conforme a la actual clasificación de información, indicaba información crítica, se cambió por restringida.
		7.3.9	Se adecua lineamiento, se cambia la unidad de reporte de mal uso de información de “Control Interno” por “área Seguridad de Información”.
		7.3.13	Se adecua lineamiento de encriptación de equipos estableciendo que se aplica a todos los equipos destinados para el ser utilizados por usuarios.
		7.4.2	Se adecua lineamiento para complementarlo con el cumplimiento de la privacidad de datos.
		7.5.10	Se adecua punto conforme a la actual clasificación de información, se adecuo información “sensible y critica” por “restringida y confidencial”.
		7.7.3	Se adecua lineamiento, se cambia al aprobador: “Control Interno y TI” por “área Seguridad de Información”.
		7.16.2	Se adecua lineamiento, se cambia al aprobador: “Oficial de Seguridad de Información y Gobierno de TI” por “área de Seguridad de Información”.
00	13/06/2018	Todas	Esta norma se deriva de la norma ATIC_NI_002

	Nombre	Cargo	Fecha
Elaboración	Juan Carlos Lara Flores	GERENTE DE TI	20/10/2020
Revisión	Giannina Monteverde Vasquez Solis	CHIEF FINANCIAL OFFICER	02/11/2020
Aprobación	Frank Lazo Noriega	GERENTE GENERAL CUMMINS	03/11/2020