|  |  |
| --- | --- |
| 1. **INFORMACIÓN GENERAL DEL DOCUMENTO** | |
| **OBJETIVO:** | Definir parámetros y lineamentos para el uso apropiado de la información de TIMON S.A. Estas reglas se definen para proteger la información de la compañía y nuestros clientes, minimizando los riesgos que puedan llegar a afectar a confidencialidad, integridad y disponibilidad de la información. |
| **DUEÑO DEL PROCESO:** | Facilitador Jr. Tecnología |
| **ALCANCE:** | Los términos y condiciones descritos en esta política aplican a todos los colaboradores internos, consultores, contratistas y proveedores de TIMON S.A. o nuestros clientes. |
| **DEFINICIONES: N/A** | |
| **DOCUMENTOS RELACIONADOS:**  GA D 06 F 01 Reporte de Baja de Disco Duro | |
| **ASPECTOS GENERALES:**  La información y sistemas de cómputo de TIMON S.A. son activos esenciales para el desarrollo de las operaciones del negocio y su dependencia en estos activos exige que se mantengan protegidos.  La presente política define, establece y hace obligatorio el cumplimiento de las siguientes medidas apropiadas para proteger los sistemas de cómputo y de información de TIMON S.A. contra la de destrucción accidental o maliciosa, daño, modificación o revelación y para mantener los niveles apropiados de confidencialidad, integridad y disponibilidad de a información contenida en los sistemas de cómputo y de información de la organización.   1. **Principios generales**  Todos los equipos de cómputo y sistemas de información proporcionados por TIMON S.A. permanecen como propiedad exclusiva de TIMON S.A. cualquier información o propiedad intelectual creada por el usuario permanece como propiedad de TIMON S.A. y no debe de ser retirada, copiada o compartida, excepto para el cumplimiento de sus funciones y bajo autorización expresa del líder inmediato del proceso.  * 1. Los sistemas de cómputo de TIMON S.A. y toda la información contenida en ellos son activos esenciales para las operaciones de la organización y su uso inadecuado o abuso por parte de un colaborador será a discreción de TIMON S.A. objeto de acciones disciplinarias de conformidad con el procedimiento establecido por la organización   2. Los usuarios deben utilizar los sistemas de información de TIMON S.A. y los dispositivos de comunicaciones de manera apropiada, legítima y consistente con sus obligaciones, con respeto hacia los demás colaboradores, clientes y/o terceros. Estos dispositivos debe ser usados de conformidad con esta política y cualquier otra directriz, instructivo/o política estándar o procedimiento definido por TIMON S.A. para tal fin   3. Ante cualquier relación con personal externo a la organización (contratistas o proveedores) deben ser conscientes de que están actuando como representantes de TIMON S.A. y cualquier acción apropiada puede afectar la imagen comercial de TIMON S.A. involucrar contractualmente a TIMON S.A. e incurrir en obligaciones y responsabilidades por parte de la organización y del usuario.   4. El uso de los sistemas de cómputo de TIMON S.A. esta proporcionado para garantizarle a los colaboradores el desempeño de sus funciones su uso podrá tener características o uso limitado de colaboradores, según se contempla en los términos de esta política y está a la absoluta discreción de TIMON S.A. y ningún usuario puede esperar o reclamar tal uso personal como un derecho o esperar que tal uso sea privado.   5. Los usuarios de las redes de datos o recursos de cómputo de TIMON S.A. no deben deshabilitar las funciones de uso o sobrecargarla mediante ejecución de programas no autorizados o evitar cualquier sistema que este hecho para proteger la privacidad o seguridad de otro usuario.   6. Los usuarios que tengan accesos a las redes de datos o recursos de computo de TIMON S.A. deben asegurarse que toda la información de la cual pueda requerirse retención de acuerdo a con la legislación vigente o en términos de las políticas de retención de documentos de TIMON S.A. sea realizado tal y como se encuentra definido.   7. Los colaboradores de TIMON S.A. deben de garantizar la complejidad y confidencialidad de las diferentes contraseñas de los sistemas de información.   8. El colaborador y/o usuario se compromete a no divulgar la información suministrada por la organización por ningún medio electrónico. Magnético u otros. En consecuencia se obliga a no utilizar los sistemas de información y/o cómputo para ningún objeto diferente al adelantar las tareas que se deriven directamente del cumplimiento del vínculo contractual adquirido con la organización.   9. Cualquier equipo portátil al ser retirado de manera temporal de la organización o traslados hacia otra sede, cliente o proveedor deberá cumplir la política de cifrado del disco y con los requisitos de seguridad de la información definidos en el instructivo para el control de equipos portátiles.   10. Se le dará un tratamiento al uso final de Los discos duros, ya que estos dispositivos guardaron información de la organización, en su vida útil, el cual tecnología garantizara la inutilidad del mismo, se diligenciara el Formato GA D 06 F 01 Reporte de Baja de Disco Duro, para llevar a cabo la baja, que contendrá como mínimo una imagen de este dispositivo digital o impreso  1. **Uso de computador**    1. En la oficina/uso general       1. Varios aspectos de la comunicación están protegidos por derechos de propiedad intelectual, que son infringidos al copiar información. Descargar, copiar, poseer y distribuir material de internet puede ser una infracción a los derechos de autor o a otros derechos de propiedad intelectual, los usuarios de las redes o recursos de computo de TIMON S.A. no deben descargar o distribuir software o información protegidos por derechos de autor o de uso no autorizado. Cualquier software o archivos descargados pueden ser usados solamente en una forma consistente con su licencia o derechos de autor, en caso de duda los usuarios deben contactar a Tecnología antes de descargar cualquier información.   El uso indebido de la información confidencial de la organización será considerado como acto de competencia desleal por lo cual el usuario quedara sujeto a las sanciones legales respectivas. De igual forma, constituirá competencia desleal y violación de la presente política la realización de los actos que se indican en el art 262 de la decisión 486 de 2000 de la comisión de la comunidad andina.   * + 1. Los usuarios no deben de acceder, descargar o distribuir cualquier material que pudiera ser considerado pornográfico, racista, sexista u ofensivo de cualquier otro modo. Esta expresamente prohibido mostrar cualquier imagen o documento ofensivo o sexualmente explicito en un sistema de información o documentación de TIMON S.A.   Adicionalmente, material ofensivo o sexualmente explicito no puede ser archivado, guardado, distribuido, editado o registrado en la red en los recursos de cómputo y sistemas de información de TIMON S.A.   * + 1. Los usuarios de las redes de datos o recursos de cómputo de TIMON S.A. no deben intentar tener acceso a segmentos o grupos restringidos de la red o acceder a información de la cual se tiene conciencia que es de carácter confidencial.     2. Los usuarios de los recursos de computo de TIMON S.A. no deben de intentar examinar, escanear o violar la seguridad de la mediadas de autenticación de un sistema o red ni interna ni externamente usando los recursos propios o de TIMON S.A.     3. El colaborador usara y navegara en las redes y recursos de computo de TIMON S.A. bajo su responsabilidad y en las condiciones, límites y horarios que determine el contrato laboral.     4. El usuario en ningún caso y bajo ninguna circunstancia utilizara las redes de datos o recursos de computo de TIMON S.A. para interceptar comunicaciones, realizar accesos no autorizados a los sistemas de información de la organización o de cualquier persona o permanecerá en ellos abusando de su cargo o extralimitándose en sus funciones.     5. Los usuarios de las redes y recursos de computo de TIMON S.A. no deben propagar a sabiendas ningún virus, gusano informativo, caballo de troya, programas- trampa o código similar. Si tal virus, gusano, caballo de troya programa trampa o código similar es descubierto por el usuario el ella debe dejar de usar el sistema inmediatamente y reportar el descubrimiento inmediatamente al centro de atención tecnología.     6. Los usuarios de recursos de computo de TIMON S.A. no deben instalar hardware o software no autorizado.     7. Los usuarios no deben prestar su nombre de usuario y/o contraseña, dado que son usuarios únicos y serán los únicos responsables por la actividades realizadas bajo su nombre de usuario y contraseña en cualquier sistema de información al cual se le haya otorgado acceso, quien incumpla con esta norma sera causal de acciones disciplinarias.     8. Los usuarios de las redes de datos o recursos de cómputo de TIMON S.A. no deben poseer herramientas, software o código (incluyendo software para rastrear archivos o detector contraseñas)que habiliten a un usuario a evitar la seguridad de un sistema de computo.     9. Los usuarios de los recursos de computo de TIMON S.A. deben tomar las medidas adecuadas para proteger la seguridad física de los recursos de computo en su posesión, asegurándose de que los dispositivos portátiles estén protegidos lógicamente (encriptar) y físicamente (guayas de protección) cuando no estén en uso y que las estaciones de trabajo estén bloqueadas cuando se dejen sin atender. Las contraseñas deben ser mantenidas confidencialmente.     10. Ningún colaborador a excepción del personal autorizado expresamente por el proceso de seguridad de la información podrá hacer uso del usuario y/o perfil de administrador local en los equipos computo de TIMON S.A.   Cualquier colaborador que llegara a necesitar este tipo de acceso deberá generar una solicitud, con la aprobación del líder inmediato en la cual se especifiquen las razones técnicas para solicitar el nivel de acceso de administrador en el equipo de cómputo asignado por el proceso.   * + 1. Los usuarios deben garantizar que la información que manejan se encuentra respaldada realizando la solicitud a Tecnología y velar para que dicha información no se encuentre ni sea de fácil acceso en los equipos de compto asignados de igual forma no se deban almacenar de manera local en los equipos.     2. Solo podrá crear carpetas compartidas o accesos a la misma desde su equipo de trabajo si está expresamente autorizado por el líder inmediato del proceso para hacerlo.     3. Está prohibido el ingreso a las instalaciones de equipos que permitan el almacenamiento de datos (computadores, Tablet, memorias o discos duros) excepto si se encuetra expresamente autorizado por el proceso de seguridad.   1. **En el hogar**      1. Los colaboradores a los que se les proporcionen recursos computacionales de TIMON S.A. para uso en el hogar deben tomar precauciones adicionales para asegurar la confidencialidad y la integridad de la información de la organización tales como: * Asegurar que los dispositivos móviles, incluyendo portátiles estén asegurados adecuadamente lógicamente (encripcion) y lógicamente (guaya de protección ) y no se dejen a la vista en lugares públicos o vehículos particulares. * Asegurar que la información confidencial de TIMON S.A. no sea vista involuntariamente por terceros (por ejemplo uso de portátiles en transportes públicos y salas de espera de los aeropuertos). * Atacar todos los aspectos de esta política  1. **Uso de correo electrónico y sistemas de mensajes**    1. Uso de negocio       1. Los usuarios deben tener particular cuidado al usuario del correo electrónico como medio de comunicación debido a que todas las expresiones de hecho, intención u opinión en un correo electrónico pueden obligar al usuario y/o a TIMON S.A. , y pueden ser exhibidas en la corte en la corte en la misma forma que otros tipos de declaraciones escritas.       2. los usuarios no deben enviar mensajes de correo electrónico, archivos adjuntos a correos electrónicos o mensajes instantáneos que puedan ser interpretados como difamatorios, atormentantes u ofensivos de alguna otra forma. Esto incluye el uso de irreverencias, obscenidades o comentarios despectivos en relación con los colaboradores, clientes u otros.       3. Los usuarios no deben de enviar o recibir archivos adjuntos vía mensajería instantánea 2. **MEDIDAS DISCIPLINARIAS ASOCIADAS AL INCUMPLIMIENTO DE LOS DIRECCIONAMIENTOS ESTABLECIDOS**   Es responsabilidad del líder del proceso de Tecnología, informar a la Gerencia, cuando se evidencie que algún funcionario está incurriendo en el incumplimiento de la misma, este funcionario será remitido a Comité de Responsabilidades, donde se determinaran las medidas disciplinarias pertinentes. | |

|  |  |  |
| --- | --- | --- |
| 1. **CONTROL DE CAMBIOS** | | |
| **Versión** | **Modificación** | **Fecha** |
| 1 | Elaboración del documento | 26/Oct/2013 |
| 2 | Se incluye actividad 1.11 para aseguramiento de la información y se crea formato como soporte de la actividad | 10/Nov/2014 |