Garantías Comunitarias®

Innovación en Riesgo

MANUAL DE POLÍTICAS DE SEGURIDAD PLATAFORMA TECNOLÓGICA

TABLA DE CONTENIDO

INTRODUCCIÓN

INTRODUCCIÓN

La Política de Seguridad de la entidad busca evitar que las amenazas latentes en el entorno, puedan acceder, manipular o deteriorar la información que en ella exista y disminuir la posible pérdida de la misma.

Este documento contiene Las Políticas de Seguridad de la Información de la entidad, basadas en buenas prácticas que expresan su interés de minimizar los riesgos y donde existe el compromiso de velar por la confidencialidad, integridad y disponibilidad de la información.

A. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

1. ACCESO A LA INFORMACIÓN

• Todos los recursos proporcionados para soportar la ejecución normal de las actividades y el procesamiento de la información, son propiedad de la entidad y deben ser usados para propósitos del negocio.

• La divulgación de información generada en la entidad, está sujeta al estudio y aprobación por parte de cada propietario de la misma.

• No divulgar información confidencial de la entidad a personas no autorizadas.

• No deberá existir sobre los escritorios, a la vista de cualquier persona, información confidencial o de importancia para la entidad.

• Las impresoras deben estar atendidas siempre, sobre todo cuando se está imprimiendo (o se va a imprimir) información confidencial de la entidad.

• El acceso a los recursos de información de la entidad, presupone la aceptación del presente documento de políticas de seguridad, el cual se encuentra ratificado a través de la firma de un acuerdo de responsabilidad que hace parte del contrato de trabajo de cada empleado.

• Los usuarios no deben copiar a un medio removible (USB, DVD o cualquier otro medio que pueda transportar información), el software o los datos residentes en los computadores de la entidad, sin la previa autorización del dueño de la información, la cual debe ser remitida al analista de seguridad de la Información para su custodia.

• En la entidad se han determinado tres niveles para la clasificación de la información (Pública, Restringida, Confidencial) y de acuerdo con esto, se determinaron los accesos (Propietario, Custodio y Usuario). Esta clasificación estará debidamente documentada y a disposición de los empleados para su consulta.

Pública: información que el Presidente/Nodo ha declarado de conocimiento público. Esta información puede ser entregada o publicada sin restricciones a los empleados o al público en general, sin que esto implique daños a terceros ni a las actividades o procesos de la Entidad.

Restringida: información que sólo puede ser utilizada por un grupo de empleados para realizar sus labores y que no puede ser conocida por otros empleados o terceros sin autorización del propietario de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma siginificativa a terceros o a las actividades y procesos de la entidad.

Confidencial: es toda aquella información que no debe ser revelada a terceros sin previa autorización del Presidente/Nodo, ya que puede representar un alto riesgo para la entidad, sus empleados y/o demás partes interesadas, con efectos catastróficos para las actividades y sus procesos.

Atendiendo lo dispuesto en el artículo 15 de la Constitución Política de Colombia y sin perjuicio de lo establecido en el numeral 4 capítulo noveno de la Circular Externa de la Superintendencia Financiera de Colombia 052 y demás normas aplicables sobre la materia, se considerará confidencial para efectos de la aplicación del presente capítulo, toda aquella información amparada por la reserva bancaria V. gr. número de cuenta, número de identificación personal (PIN), número de tarjeta física, información sobre depósitos o inversiones de cualquier tipo, créditos, saldos, cupos y movimientos de cuenta, siempre que vayan acompañados del nombre o número de identificación del cliente. Las entidades podrán clasificar como confidencial, otro tipo de información. Procedimiento 2 Gestión Documental, ver también políticas de seguridad de la información.

2. USO DE CONTRASEÑAS

• Todas las personas deben tener acceso a la información necesaria para el desarrollo de sus funciones. Dicho acceso se otorga con base en el principio del menor privilegio, es decir, las personas tienen acceso a la información y recursos que requieran según su función, sin privilegios o acceso adicionales.

• Para el acceso a cualquier sistema de información, se debe contar con usuario y contraseña personal y con el perfil necesario para la labor a desempeñar en el mismo (creación, modificación, consulta) el cual debe ser aprobado por el dueño de la información.

• Se debe evitar el uso de contraseñas compartidas, genéricas o para grupos.

• Las claves asignadas para ingresar a los sistemas de información son de uso personal e intransferible y las acciones realizadas con estas, sonresponsabilidad de cada usuario.

• Los empleados deben cambiar la clave cada vez que el sistema se lo solicite o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

• Cuando el empleado deja el puesto de trabajo, el equipo debe ser bloqueado inmediatamente.

• Los usuarios no deben aceptar que otro usuario les revele su (s) clave(s) de acceso a los sistemas, datos, correo, aplicativos y demás.

• Si alguien visualiza clave u otro tipo de información accidentalmente, debe informarlo de manera inmediata.

3. HARDWARE Y SOFTWARE

• Sólo las personas autorizadas por la Plataforma Desarrollo, serán las encargadas de realizar instalaciones de software o hardware en equipos o máquinas pertenecientes a la entidad, garantizando así las debidas licencias.

• Queda estrictamente prohibido el uso de aplicaciones tipo download (software que sirve para descargar música, videos, y en general información tipo multimedia) tales como kazaa, napster, emule, edonkey, entre otros.

• Queda prohibido descargar programas, archivos y/o información de fuentes no confiables o sospechosas.

• No utilizar los recursos informáticos (hardware, software u otros) para otras actividades que no estén directamente relacionadas con el trabajo de la Entidad.

• Debe respetarse y no puede ser modificada la configuración de hardware y software establecida por la Plataforma Desarrollo. En caso de detectarse una debilidad, se debe informar inmediatamente.

4. VIRUS

Tener la red libre de código malicioso que pueda afectar la integridad, disponibilidad y confidencialidad de la información"

• Los usuarios de cada uno de los Sistemas de información, son responsables de reportar inmediatamente en caso de encontrar situaciones sospechosas en el sistema, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades anormales.
• Siempre que se requiera del uso de USB u otros medios de almacenamiento en cualquier computador de la Entidad, debe verificarse previamente que están libres de virus u otros agentes dañinos.
• Cualquier equipo que se conecte a la red, debe ser escaneado con un sistema antivirus actualizado antes de tener acceso a la misma. El sistema operativo deberá estar actualizado.

5. COPIAS DE SEGURIDAD

• Cada usuario es responsable por la ejecución de la copia de respaldo de información (documentación, presentaciones, correo electrónico, entre otros) de su computador de trabajo.

• Los líderes deben velar porque los procesos de información que se realizan en sus áreas, tengan un respaldo de la información y por lo tanto deben solicitar a la Plataforma Desarrollo la confirmación de la misma.

6. CORREO

Para el uso de este medio de comunicación, todos los empleados deben considerar los siguientes lineamientos:

• La información confidencial de los clientes no podrá ser remitida a través de servicios gratuitos de correo electrónico tales como hotmail, yahoo, u otro.

• En caso de requerirse remitir la información confidencial de los clientes, siempre debe viajar cifrada.

• Nunca se deben ejecutar archivos que vengan adjuntos en mensaje de correo cuya procedencia es desconocida, sospechosa o poco confiable y deben ser eliminados.

• Está restringido el uso de archivos adjuntos con extensiones .pfi, .exe, .pif y .scr., así como utilizar como repositorio para archivos de música, la cuenta de correo.

7. INCIDENTES

• Ningún usuario está autorizado para probar debilidades en los sistemas. La entidad realizará evaluaciones periódicas de seguridad para probar la efectividad de las medidas implementadas. Dichas evaluaciones están enmarcadas en un plan de la entidad y son de competencia exclusiva de la Red Tecnológica.

• Todo el personal de la entidad debe vigilar los incidentes o debilidades de seguridad que puedan presentarse y reportarlos de manera inmediata al área de tecnología para su evaluación, análisis de impacto e implementación de soluciones.

8. CONTRATOS

• Toda persona contratada por la entidad debe firmar y aceptar el cumplimiento de las Políticas de Seguridad de la Información y todas las responsabilidades que se desprenden frente al tema de seguridad.

• Todos los empleados de la entidad deben participar de las actividades de sensibilización y capacitación en materia de seguridad de la información a las cuales sean convocados.

• Todo empleado que tenga bajo su responsabilidad un proveedor, es responsable de conocer los lineamientos de seguridad que se establecieron en la contratación y reportar cualquier situación que considere que atente contra la seguridad.

• Una vez terminado el contrato con un empleado, se le deben eliminar todos los privilegios que tenga en la red o cualquier sistema al que tenga acceso siguiendo el procedimiento definido.

• El responsable del proveedor deberá informar la terminación del proyecto o contrato para que le sean eliminados los privilegios asignados.

9. NORMATIVIDAD

• La ley y la normatividad interna se deben cumplir de manera estricta. Se debe tener especial cuidado con las disposiciones referentes a información de la entidad, información de clientes y propiedad intelectual.

• Todos los empleados que por su rol tengan información relacionada con los clientes, proveedores o los mismos empleados serán responsables de protegerla.

• Los lineamientos que tenga la entidad para el acceso y uso de la información con derechos de propiedad intelectual, deben ser cumplidos por los empleados y proveedores.

• Se deben elaborar acuerdos de confidencialidad por parte de cualquier empleado de la entidad, en aquellos casos en los cuales resulte indispensable suministrar información privilegiada a proveedores, terceros u otra persona que en condiciones normales no tienen acceso a la misma.

B. POLÍTICAS DE SEGURIDAD DE TECNOLOGÍA INFORMÁTICA

1. SOFTWARE

1.1. CONTROL DE VERSIONES

Se deberá seguir la metodología formal para el proceso de adquisición de software de misión crítica o prioritaria a través de terceros. Esto debe incluir un acuerdo de confidencialidad con cláusulas básicas para la protección de la información y del software, así como para la documentación y los respaldos que protejan los intereses institucionales frente a las cláusulas entregadas por el vendedor.

Adquisición de software

• En concordancia con la política de la entidad, la Plataforma Desarrollo es el área de establecer y definir técnicamente las necesidades y el ambiente de trabajo que deben suplir los nuevos sistemas informáticos que se desean adquirir.

• En cuanto al uso de software libre, deberá respetarse la propiedad intelectual intrínseca del autor.

• La Plataforma Desarrollo promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

• Todas las aplicaciones incluirán como parte de su registro, el número de versión que le corresponde y será debidamente registrado en la base de datos de configuraciones.

• La entidad respetará los derechos de propiedad intelectual aplicados a los programas de computador (software) y protegidos por la normatividad legal existente en Colombia y en convenios internacionales.

• El software instalado en la entidad está protegido por derechos de autor. Está prohibida su copia total o parcial en cualquier medio de almacenamiento..

Administración del Software

• La entidad debe contar en todo momento con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato. Las licencias se almacenarán bajo los adecuados niveles de seguridad e incluidas en un sistema de administración, efectuando continuos muestreos para garantizar la consistencia de la información allí almacenada.

• Los ambientes de desarrollo de sistemas, pruebas y producción, deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción, se modificarán únicamente por personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos, y se considerarán planes de contingencia y recuperación.

• Se deben establecer procedimientos para pruebas de software nuevo o modificado.

• Se deben emplear bitácoras para llevar un control a las modificaciones o actualizaciones a los sistemas operativos o software de las estaciones de trabajo y/o servidores.

• Efectuar de manera periódica respaldos de la información y mantenerlos en un lugar seguro fuera del sitio de cómputo.

• Se debe hacer copia del software original y ésta será la que se emplee para las instalaciones.

• El software original y la documentación relacionada deberá mantenerse bajo resguardo.

• No se permite la existencia de software sin licencia en los equipos.

• Se debe hacer seguimiento al uso de software, efectuando revisiones periódicas a los discos duros y sus contenidos, con el fin de evitar la existencia de software sin licencia en los mismos.

• Sólo personal autorizado por la Red Tecnológica, puede instalar software y en el caso de no ser “software de libre distribución”, este debe contar con la respectiva licencia de uso.

• Corresponde a la Red Tecnológica detallar y emitir los procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

• Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos con los que cuenta la entidad, dispongan de software de seguridad (antivirus, privilegios de acceso y otros que apliquen).

1.2. DESARROLLO DE SOFTWARE

• La entidad deberá tener una metodología formal para el desarrollo de software de los sistemas de información y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas, procedimientos, controles y estándares aplicables en el desarrollo de sistemas.

• Adicionalmente, toda solicitud de modificación al software deberá contar con estudios de factibilidad y de viabilidad, al igual que las autorizaciones respectivas dentro de la entidad.

• Con el propósito de garantizar integridad y confidencialidad de la información que administrará el software desarrollado y antes del paso a pruebas, se deberán ejecutar las pruebas intrínsecas al desarrollo y a la documentación técnica respectiva.

• Para todo desarrollo de software se deberán utilizar herramientas, de las cuales se tengan certeza que su comportamiento es seguro y confiable. Solamente las funciones descritas en el documento aprobado de especificaciones de la solución tecnológica, podrán ser desarrolladas.

• Los programadores de software no deberán conocer las claves utilizadas en ambientes de producción (encriptores, administradores u otras).

• Los desarrollos y/o modificaciones hechos a los sistemas de aplicación, no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento, operación y de seguridad adecuados. La suficiencia de este material, deberá ser determinada por los usuarios responsables en la entidad.

Implantación del Software

• Las características que son innecesarias en el ambiente informático de la entidad se identificarán y desactivarán en el momento de la instalación del software.

• Antes de implementar el software en producción, se verificará que se haya realizado: la divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de producción. La entidad deberá poseer un plan de trabajo de puesta en producción, con el fin de minimizar el impacto del mismo.

• Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, la cual en ningún momento deberá ser el área de desarrollo. Se debe cumplir con todo lo dispuesto en la catalogación de software.

• Los sistemas de información que se instalen en la entidad, deberán tener acceso controlado, los usuarios deberán identificarse con usuario y contraseña.

• Se deberá tener un inventario completo del software que es propiedad de la entidad (base de datos de software), adquirido mediante terceros y bajo licenciamiento. Las licencias deberán ser protegidas y almacenadas de forma segura y con una persona encargada de su custodia.

1.3. INSTALACIÓN

Control de copia de software registrado

• El software patentado es generalmente suministrado bajo una licencia, la cual limita el uso de dichos productos en equipos específicos y puede limitar la copia únicamente en casos de seguridad (respaldo).

• Es política de la entidad, el cumplimiento de todas las obligaciones, evitando el duplicado de material patentado sin la autorización del propietario.

• La copia de software patentado para uso en computadores que no pertenezcan a la entidad, sin la respectiva autorización, infringe los derechos de copia y se constituirá en violación a la ley y a las políticas de la entidad.

• Si es necesario utilizar software en equipos adicionales, las licencias se deben extender y se deben adquirir copias adicionales.

• Los servidores no deben tener instalado software que no sea necesario para cumplir con las labores de los usuarios de los sistemas de información de la entidad.

1.4. RESPALDO DE DATOS

• Toda la información sensible, valiosa o crítica residente en los equipos, servidores, sistemas, discos de almacenamiento o cintas de la entidad, deben respaldarse periódicamente. La periodicidad debe estar definida de acuerdo con las necesidades de recuperación del procedimiento definido.

• Los respaldos de información sensible, crítica y valiosa, deben almacenarse en un sitio protegido y con controles estrictos de acceso fuera de las instalaciones principales de la entidad.

• Se debe verificar periódicamente, la integridad de los respaldos que se están almacenando.

• Se deben copiar a los equipos de contingencia y en la periodicidad establecida, fuentes y objetos ejecutables de las carpetas ubicadas en los equipos críticos..

• Toda la información histórica almacenada, debe contar con los medios, procesos y programas capaces de manipularla sin inconvenientes, esto teniendo en cuenta la reestructuración que sufren las aplicaciones y los datos a través del tiempo.

• La información sensible, crítica o valiosa almacenada en medios magnéticos durante tiempo prolongado, debe ponerse a prueba al menos cada 2 o 3 meses para asegurarse de que la información aún es recuperable o debe copiarse a un medio nuevo.

• Los procedimientos de almacenamiento en medios magnéticos y ópticos (DVD, cintas magnéticas, etc.) deben asegurar que la información sensible, crítica o valiosa almacenada durante tiempo prolongado, no se pierda por deterioro.

1.5. BASES DE DATOS

• Se protegerá la integridad de los datos, realizando un control de acceso a las tablas que sólo lo deben hacer los administradores autorizados y dejando registro de la actividad realizada. Se definirán los diferentes niveles de acceso, de acuerdo con el rol y la función a realizar en las bases de datos.

• La información almacenada de los usuarios estará protegida por principios de confidencialidad y por lo tanto quedará protegida de los accesos no autorizados, alteración o revelación.

1.6. MANTENIMIENTO

• El tercero designado por la entidad para el desarrollo de sistemas, no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos por la entidad. A su vez, ésta contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

• Para cada mantenimiento a la versión del software de misión crítica y prioritaria de la entidad, se actualizará el depositado en custodia en el sitio alterno y el respaldado en la institución. Este software y su documentación, se verificarán y certificará su actualización.

• No se deben hacer cambios al software de producción, sin las debidas autorizaciones por escrito por parte de la Plataforma Desarrollo y sin cumplir con los procedimientos establecidos por la entidad. A su vez, ésta contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

• La documentación de todos los cambios hechos al software, se preparará simultáneamente con el proceso de cambio. Se debe considerar, además, que cuando un tercero efectúe ajuste al software de la entidad, éste deberá firmar un acuerdo de no-divulgación y no utilización del mismo sin autorización.

1.7. PRUEBAS

• Todo sistema deberá ser probado antes de ponerse en ambiente de producción y con el fin de garantizar la integridad de la información en producción, ésta deberá ser debidamente planeada, ejecutada, documentada y controlada. Además, el ambiente de pruebas deberá ser lo más idéntico en su configuración, al ambiente real de producción.

• Las pruebas sobre el software desarrollado deberán contemplar varios aspectos funcionales y técnicos.

• Adicionalmente, se debe revisar cuidadosamente la documentación requerida, así como la revisión de los procesos de retorno a la versión anterior.

2. HARDWARE

2.1 USO

El objetivo de esta política es evitar daño, pérdida o puesta en peligro de los activos relativos a la información e interrupción de las actividades de la Entidad.

• Las medidas de seguridad de la información que se considerarán al poner esta política en ejecución, comprenden el acceso ilegal que se puede tener con el objetivo de hurto, daño o interrupción de las operaciones. Los computadores y todos los sistemas de comunicación se deben salvaguardar contra la intrusión física ilegal y desautorizada.
• Las instalaciones de tecnología están para el propósito del negocio. Cualquier uso de las instalaciones para propósitos no autorizados (sin la aprobación de la Presidencia), se puede considerar como uso inadecuado de los recursos de la entidad, acarreando la acción disciplinaria apropiada.
• Debe respetar y no modificarse la configuración de hardware y software establecida por la Red
• Deben protegerse los equipos de riesgos del medio ambiente (polvo, fuego y agua). Tecnológica.
• Deben usarse protectores contra descargas transitorias de energía eléctrica y en los servidores deben usarse fuentes de poder in-interrumpibles (UPS).
• Cualquier falla en los computadores o en la red, debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
• Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Además en caso de suceder algo inesperado de este tipo, debe reportarse de manera inmediata a las Plataformas Desarrollo y Estratégica.
• Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del protector de pantalla.
• Cuando ya no sean necesarios o útiles los datos confidenciales, se deben cerrar o eliminar
• El personal no tiene permitido ingresar al sitio de trabajo, computadores portátiles (laptops). y en caso de ser necesario se requiere de la autorización correspondiente.
• Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs (internet inalámbrico u otro) que tengan también conexión a la red local (LAN), a menos de que sea debidamente autorizado.
• Todas las comunicaciones de datos deben efectuarse a través de la LAN de la entidad.
• El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.
• Los empleados deben reportar a la Plataforma Desarrollo de la entidad, sobre daños o pérdida del equipo que tengan asignados y no realizar intervención directa para reparar el equipo, lo cual está expresamente prohibido. La entidad proporcionará el personal interno o externo para la solución del incidente reportado.
• Todos los equipos deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación. Éste debe ser actualizado de forma periódica por el área encargada y dependiendo del tipo de equipo (computadores, servidores u otro).
• El hardware que adquiera la entidad en su totalidad, debe tramitarse a través de canales de compra estándares y debidamente certificados.
• Para cualquiera de los equipos y sistemas de comunicación utilizado en los procesos de producción de la entidad, se debe aplicar el procedimiento de control de cambios, que garantice que sólo se realicen aquellos autorizados. Este procedimiento debe incluir documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la descripción del cambio realizado.
• Todos los productos de hardware deben ser registrados por el proveedor y deben contar con el respectivo contrato de mantenimiento.
• Los equipos de cómputo que soportan la infraestructura tecnológica, no deben moverse o reubicarse sin la aprobación previa de la Red Tecnológica.
• Los equipos deben ubicarse en lugares donde se minimicen los accesos de las personas a dichas áreas de trabajo.
• Los equipos de procesamiento y almacenamiento de la información que manejen datos sensibles, se deben instalar donde se reduzca el riesgo de que otros vean los procesos durante su uso.
• Los elementos que requieran protección especial, se deben aislar para reducir el nivel general de protección requerido.
• Se deben adoptar medidas para minimizar los riesgos de posibles amenazas como: robo, incendio, explosivos, humo, agua, polvo, vibraciones, agentes químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas.
• Se deben monitorear las condiciones ambientales que puedan afectar negativamente el funcionamiento de los equipos de procesamiento de información.

2.2 MANTENIMIENTO

• Los cambios de partes en los equipos de cómputo deben ser evaluados y autorizados por la Plataforma Desarrollo.
• Los equipos y sistemas de comunicación utilizados en los procesos productivos de la entidad, deben tener un procedimiento de control de cambios que garantice que sólo se aplican aquellos debidamente evaluados y autorizados.
• Se debe llevar un control anual y por escrito de los mantenimientos o inspecciones realizadas a los equipos del centro de cómputo.
• Los equipos de cómputo de la entidad no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización de la Plataforma Desarrollo.

2.3 OBSOLESCENCIA – RENOVACIÓN (TECNOLOGIA)

Disposición (retiro) de los equipos de cómputo

• Todos los elementos que contengan capacidad de almacenamiento (ej. discos duros fijos), se deben chequear para asegurarse de que información sensible y software bajo licencia, se haya descargado ó sobrescrito antes de disponer de él. La información de la entidad se puede comprometer si no se es cuidadoso cuando se retira de servicio un equipo de cómputo.

• Los dispositivos de almacenamiento defectuosos que contengan información muy sensible, pueden requerir de una evaluación de riesgo para determinar si el dispositivo se deba destruir, reparar o eliminar.

3. CENTRO DE CÓMPUTO

3.1 SEGURIDAD.

Para el Centro de Cómputo de la entidad aplicarán TODAS las políticas mencionadas en el CAPÏTULO IV. ESTÁNDARES del presente documento.

3.2 OPERATIVIDAD.

• Las personas designadas para la administración del centro de cómputo, se guiarán por la adecuada segregación de funciones descritas en el perfil de su cargo.
• La ejecución de procesos, operación de los equipos y de todo el procesamiento de datos, debe estar debidamente documentada.
• Se hará seguimiento sobre la correcta ejecución, administración y control de procesos y la adecuada detección y corrección de errores.
• Se generarán informes periódicos sobre las labores de administración del centro de cómputo, de los equipos y de los recursos de procesamiento de la información.
• El control de acceso se hará mediante planilla.
• El centro de cómputo debe tener los mínimos estándares de calidad en cuanto a dispositivos de seguridad se refiere: transformador de aislamiento, UPS, redundancia en los servidores de misión crítica, planes de contingencia con los proveedores y comunicaciones, entre otros.

3.3 MONITOREO

• La Red Tecnológica realizará copias de seguridad diarias de las bases de los aplicativos que están en producción y soportan la operatividad del negocio, para garantizar la continuidad del mismo.
• La Red Tecnológica debe crear medios magnéticos con las copias tomadas de las bases de datos de producción y enviarlas a custodia en almacenamiento externo cada semana para salvaguardar la información sensible de la entidad.
• La Red Tecnológica debe brindar la infraestructura necesaria creando ambientes alternos a las bases de datos de producción para el desarrollo de mejoras en los aplicativos.
• Los perfiles de usuario para el acceso remoto a los servidores deben estar configurados como usuarios de escritorio remoto, para así restringir los permisos sobre dicho perfil.
• Los servidores no deben tener instalado software que no sea necesario para cumplir con las labores de los usuarios de los sistemas de información de la entidad.

3.4 ALTA DISPONIBILIDAD

• Se deberá garantizar la disponibilidad de equipos 24 horas 7 días a la semana.
• Se garantiza la disponibilidad de personal para el manejo de los equipos 24 horas 7 días a la semana.
• Se debe garantizar que SÓLO el personal necesario para la activación del centro de cómputo alterno, tenga acceso a dichas instalaciones.
• Garantizar en forma continua, la disponibilidad de los servicios ofrecidos a todos los usuarios de la red..
• Cualquier falla en los computadores o en la red, debe reportarse inmediatamente a la extensión 105, ya que podría causar problemas serios como pérdida de la información o generar la no disponibilidad de los servicios.
• El centro de cómputo deberá garantizar la mayor disponibilidad en sus servicios y contar con una bitácora con registros de fallas, problemas, soluciones y acciones desarrolladas.

4. ESTÁNDARES

4.1 ANTIVIRUS

Control de Virus

• La Red Tecnológica suministra un sistema antivirus, el cual debe estar instalado en cada estación de trabajo y en los servidores, funcionalidad que los usuarios no deben desactivar de sus equipos.

• La responsabilidad de evaluar la posible existencia de virus en forma adecuada y con el software anti-virus en toda la información que provenga de Internet, recae directamente sobre el usuario. Este proceso debe ser realizado antes de abrir o ejecutar los archivos así como antes de divulgarlos a través de la red, con el fin de no propagar virus informáticos u otros programas.

• Los usuarios deben notificar inmediatamente al área de tecnología si tiene alguna sospecha de que existe un virus en la red pública.

• Los computadores portátiles, laptops y cualquier equipo que se pueda conectar a la red de la entidad, deben estar protegidos con sistemas antivirus actualizados para minimizar el riesgo de propagación de virus y software mal intencionado o ser escaneados con un programa antivirus antes de conectarse a la misma.

• Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente como evento de riesgo y poner el equipo en cuarentena hasta que el problema sea resuelto.

4.2 FIREWALL Y RED

• Como parte de la solución de seguridad, se debe emplear un firewall y éste debe ser el único punto de acceso entre la red interna y las redes externas. Esto aplica tanto para el sitio principal, como para el alterno.
• Todos los elementos de red y comunicación como los servidores, los sistemas operativos y los aplicativos de software, deben estar siempre configurados de manera que busque conservar los atributos de seguridad de la información que procesan, protegiéndolos del acceso no autorizado y lógico. Se deben realizar todas las actividades rutinarias sobre la infraestructura tecnológica que busquen asegurar que no se degraden los atributos de seguridad de los mismos.
• Los usuarios podrán utilizar libremente los servicios de red (Internet, archivos, antivirus, correo, agenda y aplicativos administrativos). Sin embargo en caso de ser necesario, la Red Tecnológica podrá proponer restricciones de acceso a ciertos servicios, en procura de mejorar el rendimiento de la red.

Red WAN Y VPN'S

• El diseño de la red WAN, deberá tener en cuenta la demanda de tráfico, número de usuarios, necesidades de disponibilidad y criticidad, la tecnología de transporte a implementar, el ancho de banda en los canales y esquemas de redundancia y respaldo.
• La Red Tecnológica deberá definir el tipo de configuración de la red WAN y/o VPN: tipología de la red WAN y/o VPN, topología, medios de transmisión, cable y conectores, componentes de la red, equipos que la interconectan, protocolos de comunicación, direcciones IP y máscaras de red y clase de red.
• Se deberá tener actualizada la documentación relacionada con: diagrama topológico descriptivo de la red, indicando los puntos de cubrimiento y la manera como se encuentran interconectados los nodos de acceso, cuadro de configuración de enlaces en cuanto a velocidades, medios físicos y enlaces de respaldo, documentos de disponibilidad, niveles de ocupación de ancho de banda.
• La Red Tecnológica deberá publicar y difundir entre los usuarios de recursos informáticos a través de la red WAN y/o VPN, el "Proceso de Administración de Recursos Tecnológicos" y el "Manual de políticas, uso y administración de Recursos Tecnológicos"..
• La Red Tecnológica deberá establecer procedimientos y mecanismos de monitoreo para mejorar el desempeño de la red.
• Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en equipos de escritorio (PCs, Terminales, estaciones de trabajo y otros) que tengan también conexión a la red local (LAN o WAN), a menos de que sea debidamente autorizado por la Plataforma Desarrollo. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la entidad.

4.3. CUENTAS DE USUARIO-CONTROLES DE ACCESO

• Las palabras claves o los mecanismos de acceso que les sean otorgados a los empleados, contratistas o terceros, son confidenciales y de estricta responsabilidad de cada uno de ellos tal cual como se estipula en la vía legal y en el procedimiento de custodia de claves y/o llaves de encripción.
• Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
• El acceso físico o lógico (conexión a la red) de un tercero, conlleva riesgos a la seguridad como el posible daño o pérdida de datos. Estos riesgos se deben identificar con anticipación y las medidas de seguridad apropiadas se deben acordar con el contratista e incluir en el contrato.

Para el acceso lógico se hace necesario tener en cuenta:

- La necesidad de identificar los riesgos para la entidad.
- La necesidad de una aprobación por parte de la Plataforma Desarrollo.
- Las implicaciones en los planes para la continuidad del negocio.
- Los estándares de seguridad a especificarse y el proceso para medir el grado de cumplimiento.

• Todos los sistemas conectados a la red de la entidad, deben solicitar el log-in (acceso). Se debe buscar que información específica como el nombre de la entidad, el sistema operativo, el nombre de la aplicación y otros aspectos relevantes, no aparezcan hasta que el usuario tenga acceso exitoso al sistema.

Se debe implementar la suspensión de la sesión, cuando pase un largo período sin actividade en una aplicación (Ej. 10 minutos) y que esta se reestablezca cuando el usuario introduzca la contraseña adecuada.

• Si el usuario está utilizando información sensible clasificada como secreta o delicada, no podrá abandonar su equipo de cómputo o estación de trabajo sin antes salir de los sistemas o aplicaciones pertinentes.

Uso de la contraseña

Uso de la contraseña

Elección de contraseñas: para el buen uso de las contraseñas se debe tener en cuenta lo siguiente:

a. Longitud mínima de 8 caracteres.
b. Se deben emplear letras mayúsculas y minúsculas.
c. Se deben combinar letras, números, signos de puntuación y caracteres especiales.
d. No deben estar basados en información personal, nombres de familiares, mascotas, números de fechas conmemorativas, placas de sus vehículos, cédulas, dioses mitológicos, personajes de series o caricaturas, o lugares familiares.
e. No debe escribirla en una parte visible de su escritorio, agenda personal u otro y no debe revelarla a ninguna persona. Toda acción con una clave, está bajo la responsabilidad del usuario dueño de ésta.

Contraseñas y el control de acceso

• El usuario no debe guardar su contraseña en una forma legible en archivos en discos duros, USB o cualquier otro medio de almacenamiento magnético y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si tiene indicios de que su contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente usadas. Siempre que sea posible, se debe impedir que los usuarios vuelvan a usar contraseñas anteriores.
• Las contraseñas no se deben transmitir a través del correo electrónico o de cualquier otro medio ni se le deben revelar a otras personas.
• Las contraseñas son personales e intransferibles. El usuario no debe permitir que otros individuos usen sus cuentas y contraseñas. Quien revele a un tercero esta información, asumirá las consecuencias por las acciones que éstos hagan con dicha contraseña.
• Los empleados de la entidad no permitirán que personas diferentes a ella, obtengan acceso a los servidores o a su sistema de correo electrónico a través de su cuenta.
• Las contraseñas para acceder al sistema no deben ser fácilmente descifrables para otros. El usuario debe certificar que la definición de sus contraseñas no sea obvia y elemental.
• Está prohibido intentar entrar en el sistema por medio de la cuenta de otro empleado.
• Intentar violar los sistemas de seguridad y de control de acceso, son acciones que violan las políticas de la Entidad y son sancionadas.
• Si algún usuario tiene sospecha de que alguien ha accedido con su cuenta a los sistemas de información, debe notificarlo inmediatamente a la Plataforma Desarrollo. .
• Está prohibido compartir la contraseña.
• Es una norma tácita de buen usuario, no mirar el teclado mientras alguien digita su contraseña.
• La contraseña se debe cambiar periódicamente. Por lo menos cada 30 días.
• Las cuentas se bloquearán luego de determinado número de intentos fallidos o cuando se reporte el bloqueo de una cuenta, pueden tomarse distintas medidas:
o Enviar un mensaje al administrador y/o mantener un registro especial (el cual se activará también a través de los mismos sistemas).
o Enviar un mensaje al proceso de tecnología para constatar que personas ajenas hayan intentado utilizar indebidamente la cuenta del usuario.
• Cierta clase de información puede capturarse, grabarse y guardarse por requisitos de ley, para tener evidencias en casos de acciones disciplinarias y judiciales o cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Cuentas de los usuarios (TECNOLOGÍA)

• No debe concederse una cuenta a personas que no sean empleados de la entidad, a menos de que estén debidamente autorizados.

• Privilegios especiales tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas. Dichos privilegios deben ser ratificados cada mes.

• Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

• La solicitud de creación de cuenta de red debe realizarse por la Plataforma Estratégica a la Red Tecnológica cuando es personal nuevo, el cual determina los roles y privilegios que deben asignarse. Y cuando se deben cambiar los permisos a un usuario antiguo la Plataforma Estratégica envía correo a la Red Tecnológica con Formato aplicado.

• Las contraseñas o los mecanismos de acceso a los recursos informáticos que les sean otorgados a los usuarios, son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos de que exista un requerimiento legal o medie un procedimiento de custodia de claves. De acuerdo con lo anterior, los usuarios no deben tener contraseñas u otros mecanismos de acceso de otros usuarios que puedan permitirles un acceso indebido.

• Se prohibe el uso de cuentas anónimas o de invitado en los aplicativos administrativos. Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de los servidores y sus respectivos sistemas operativos deben entrar empleando su propio nombre de usuario (usuario).

• Toda cuenta debe ser suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 90 días.

• Para prevenir ingresos no autorizados o ataques, el número de intentos de ingresos con una contraseña, debe limitarse a 3, luego de lo cual la cuenta involucrada queda suspendida.

• Ningún usuario debe tener la clave de administrador de los equipos de escritorio, de detectarse se debe cambiar e informar a la Plataforma Estratégica para el cambio.

• Para evitar el uso no autorizado, abuso, fraude u otro acto mal intencionado que involucre los sistemas informáticos, se deben llevar logs de auditoría que contengan información detallada de las actividades realizadas.

• Los archivos de bitácora (logs) y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, son importantes para la detección de intrusos, brechas en la seguridad, investigaciones y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y sólo pueden ser consultados por personas debidamente autorizadas.

4.4 CORREO ELECTRÓNICO.

Políticas de uso del correo electrónico

• El personal del área de tecnología, no leerá o facilitará a otra persona para que lea el contenido de ningún archivo de correo electrónico del personal, sin obtener el permiso del usuario, excepto en caso que exista un motivo razonable para hacerlo. Dichos motivos pueden incluir, sin limitarse a ello, mantener la integridad del sistema (tal como la eliminación de virus), cumplir obligaciones legales y responsabilidades de la Plataforma o Red encargada. No obstante lo anterior, el jefe inmediato de los usuarios del correo electrónico o la Presidencia pueden obtener acceso a los buzones en caso de que se requieran investigaciones o en caso de emergencia (Ej. ausencia durante un período prolongado de tiempo vacaciones, debido a enfermedad u otro motivo).
• El administrador del servicio del correo electrónico no podrá interceptar, editar, monitorear o eliminar ningún mensaje de correo de ningún usuario, salvo autorización expresa de este o su superior, o en los siguientes casos:

- El usuario haya incurrido en actos ilegales.
- Requerimiento expreso de autoridades policiales o judiciales.
- Para identificar o resolver problemas técnicos.
- El mensaje comprometa el normal funcionamiento del servicio.

4.5 ENCRIPTACIÓN

• Todos los procesos relacionados con encripción de datos deben ser soportados preferiblemente por módulos de software (MD5). Este sistema minimiza la amenaza de ingeniería de reverso del software y una revelación de la(s) clave(s)
• No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
• Toda la información clasificada como restringida o confidencial que se requiera intercambiar con clientes a través de medios electrónicos, debe ser protegida para prevenir su divulgación o conocimiento por personas no autorizadas y para prevenir cualquier cambio o alteración. La protección se debe efectuar mediante controles criptográficos de cifrado y firma digital según se requiera.
• La utilización de encripción de datos y autenticación de mensajes será necesaria para proteger datos clasificados y transacciones financieras. Las tecnologías para realizar estos procedimientos serán recomendadas por el área de tecnología.

4.6 INTERNET

• El usuario no puede utilizar una conexión privada a Internet (vía telefónica, modem u otro) a través de las estaciones de trabajo conectadas simultáneamente a la red de la entidad. Es obligatoria la desconexión física y lógica de la red de la entidad cuando se utilice este medio de comunicación paralelo con el uso de las redes de la entidad y debe existir la aprobación de dicha conexión por parte de la Plataforma Desarrollo.
• Para los equipos portátiles que se utilicen para realizar conexiones a Internet (incluye las conexiones desde su sitio de residencia) donde no se puede asegurar la existencia de un Firewall, se debe tener especial cuidado de los sitios visitados en Internet.
• El material que aparezca en la página de la entidad deberá ser aprobado por la Presidencia y la Red Tecnológica, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
• No se permite la descarga de archivos como protectores de pantalla ya que pueden ser programas dañinos.
• Por ningún motivo se debe bajar información o software de Internet a menos de que haya una autorización explícita de la Plataforma Desarrollo para dicha actividad y se hayan tomado todas las previsiones del caso para la protección de los recursos contra eventuales virus y de derechos de autor.
• No está permitido suscribirse a foros ni sitios de redes sociales a nombre de la entidad. Esto puede comprometer la integridad y el buen nombre de la entidad.

4.7 POLÍTICA DE GESTIÓN DE CONTINUIDAD SERVICIOS TIC

• Preparar, implementar y mantener el Plan de Emergencia, Contingencia y de Recuperación de desastres y continuidad del negocio relacionados con tecnología informática.

• Liderar el proceso de pruebas que se debe ejecutar periódicamente a los Planes de Emergencia, Contingencia y de Recuperación.

• Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar su relevancia, efectividad, practicidad y factibilidad para llevarlo a cabo. Cada prueba debe documentarse. Los resultados y las acciones de corrección, deben comunicarse a la alta dirección.

• Es responsabilidad de la Red Tecnológica preparar, actualizar periódicamente y probar los planes de Contingencias, Emergencias y Recuperación, previendo la continuidad de los procesos críticos para el negocio en el evento de presentarse una interrupción o degradación del servicio.

• La Red Tecnológica debe establecer, mantener y probar periódicamente el sistema de comunicación que permita a los usuarios notificar posibles intromisiones a los sistemas de seguridad. Estos incluyen posibles infecciones por virus, intromisión de hackers, divulgación de información no autorizada y debilidades del sistema de seguridad.

• El plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento de la presencia de un desastre. Este debe permitir que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos del negocio, en un tiempo razonable para cada caso y contemplando como mínimo, los riesgos más probables de ocurrencia.

• El mantenimiento del plan de Contingencias y Recuperación general, debe incluir entre otros, un proceso estándar que integre los planes de contingencia para computadores y comunicaciones, así como también el inventario de hardware, software existente y los procesos que correrán manualmente por determinado tiempo.

GLOSARIO

CRITERIOS DE SEGURIDAD

Basados en la circular externa 052 de octubre de 2007, emitida por la Superintendencia Financiera de Colombia, tenemos:

Confidencialidad: la información debe ser conocida exclusivamente por las personas autorizadas, en el momento y forma prevista.

Integridad: la información tiene que ser completa, exacta y válida, siendo su contenido el previsto de acuerdo con unos procesos predeterminados, autorizados y controlados.

Disponibilidad: la información debe estar accesible y ser utilizable por los usuarios autorizados en todo momento, debiendo estar garantizada su propia persistencia ante cualquier eventualidad.

DEFINICIONES

Amenazas: cualquier acción o evento que puede ocasionar consecuencias adversas.

Ataques: tipos y naturaleza de inestabilidad en la seguridad.

Autorización: lo que se permite cuando se ha otorgado acceso.

Control de acceso: limitar el acceso autorizado sólo a entidades autenticadas.

Controles: cualquier acción o proceso que se utiliza para mitigar el riesgo.

Contra medidas: cualquier acción o proceso que reduce la vulnerabilidad.

Estándar: regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Sirven como especificaciones para la implementación de las políticas.

Evento de seguridad: es la ocurrencia identificada de un estado del sistema, servicio o red, que indica una posible violación a la política de seguridad, una falla de las salvaguardas, o una situación desconocida que puede ser relevante para la seguridad.

Impacto: los resultados y consecuencias de que se materialice un riesgo.

Incidente de seguridad: es toda aquella violación a las políticas de seguridad, fallas de los sistemas y pérdida del servicio, errores por datos incompletos e inexactos, fallas en procesos, violaciones a la confidencialidad e integridad de la información, entre otros.

Incidentes sobre virus: es una ocurrencia simple de uno o varios archivos infectados por un virus en un computador o servidor. Cuando los virus reaparecen después de haberlos limpiado, se considerarán un nuevo incidente.

Normas: establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

Políticas: declaración de alto nivel sobre la intención y la dirección de la gerencia.

Vulnerabilidades: deficiencias que pueden ser explotadas por amenazas.

VERSIÓN ANTERIOR	NATURALEZA DEL CAMBIO	VERSIÓN ACTUAL
00	Versión inicial para el Sistema de Gestión de GCG	01