2014

POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN RELATIVOS A TERCEROS PRESTADORES DE SERVICIOS

VICEPRESIDENCIA DE TIC

POSITIVA COMPAÑÍA DE SEGUROS S.A.

Marzo de 2014

Introducción ___ *3*

Políticas de seguridad de la información relativas a terceros prestadores de servicios de Información ___ *3*

a. Política de Seguridad de la Información ___ **3**

b. Política de Organización de la Seguridad de la Información ___ **4**

Estándares asociados a esta política ___ *5*

1. Estándar de acuerdos de Nivel de Servicio ___ 6
2. Estándar de Contratación con terceros ___ 6
3. Estándar de requerimientos de seguridad con terceros ___ 7

c. Política de Seguridad Física y Ambiental ___ **8**

d. Estándares asociados a esta política ___ **9**

1. Estándar de Seguridad de los Equipos ___ 9
2. Estándar para el control de Acceso Físico ___ 10
3. Estándar de instalación y desinstalación de software y hardware ___ 11

e. Política de Cumplimiento de requisitos legales en TI ___ **11**

Estándares asociados a esta política ___ *11*

1. Estándar de Contratación con terceros ___ 11
2. Estándar de Requisitos legales y normativos ___ 11

f. Política de Gestión de Activos de Información ___ **12**

Estándares asociados a esta política ___ *12*

1. Estándar de Etiquetado de Información ___ 12

g. Política de Adquisición, desarrollo y mantenimiento de Sistemas. ___ **13**

Estándares asociados a esta política ___ *13*

1. Estándar de control de versiones de Software ___ 13
2. Estándar de control de cambios en SI ___ 13
3. Estándar de enmascaramiento de datos ___ 13
4. Estándar de Ejecución de Proyectos ___ 14
5. Estándar de gestión de configuración ___ 14
6. Estándar de Gestión de Vulnerabilidades Técnicas ___ 14
7. Estándar de implantación y aceptación de sistemas ___ 14
8. Estándar de Migración de Datos ___ 14
9. Estándar de seguridad de los sistemas de Información ___ 15

h. Política de Gestión de Comunicaciones y Operaciones ___ **16**

Estándares asociados a esta política ___ *17*

1. Estándar de Administración de entrega de servicios a terceros ___ 17
2. Estándar de control de cambios en sistemas de información ___ 18
3. Estándar para controles de red ___ 18
4. Estándar de control de versiones de Software ___ 18
5. Estándar de gestión de configuración ___ 18
6. Estándar de implantación y aceptación de sistemas ___ 18
7. Estándar para el Manejo de Medios de la Información e Intercambio de Información ___ 18
8. Estándar para la Protección contra software malicioso y códigos móviles. ___ 19

i. Política de Control de Acceso de TI _____ 20

Estándares asociados a esta política _____21

1. Estándar de control de Acceso Lógico_____21

j. Política de Gestión del Riesgo en TI _____ 21

k. Política de Seguridad de la Información Frente al Recurso Humano _____ 22

l. Política de Gestión de Incidentes de TI _____ 23

Estándares asociados a esta política _____24

1. Estándar de Gestión de Incidentes _____24

m. Política de Gestión de Continuidad del Negocio en TI _____ 24

Introducción

La Contraloría General de la Nación en el año 2012 recomendó a la Vicepresidencia de Tecnologías de la Información y Comunicaciones hacer una revisión de las políticas de seguridad implementadas por POSITIVA S.A., para el manejo de la información de la compañía por parte de terceros prestadores de servicios. Esta labor se adelantó con el propósito de verificar la correcta aplicación de las políticas de seguridad de la información que deben regir los acuerdos de servicio con estos terceros, incorporando las mejoras prácticas dentro de los acuerdos contractuales definidos con estos proveedores.

Políticas de seguridad de la información relativas a terceros prestadores de servicios de Información

Se identificaron las políticas de seguridad de la información de POSITIVA S.A. que tienen que ver con el manejo de activos de información por parte de terceros prestadores de servicios, las cuales se relacionan a continuación:

a. Política de Seguridad de la Información
b. Política de Organización de la Seguridad de la Información
c. Política de Seguridad Física y Ambiental
d. Política de Cumplimiento de requisitos legales en TI
e. Política de Gestión de Activos de Información
f. Política de Adquisición, desarrollo y mantenimiento de Sistemas.
g. Política de Gestión de Comunicaciones y Operaciones
h. Política de Control de Acceso de TI
i. Política de Gestión del Riesgo en TI
j. Política de Seguridad de la Información Frente al Recurso Humano
k. Política de Gestión de Incidentes de TI
l. Política de Gestión de Continuidad del Negocio en TI

(*) Se aclara que el total de las Políticas de Seguridad de la Información de POSITIVA, se encuentran en la organización y pueden ser solicitadas cuando el tercero lo estime conveniente.

Se analizó cada política y sus estándares, en los temas relacionados con contratación y manejo de información, para lo cual se detalla el siguiente análisis:

a. Política de Seguridad de la Información

Esta política define la adopción por parte de POSITIVA S.A., de las políticas y controles de seguridad de la información, expuestas en la norma ISO 27000.

La política define la obligatoriedad de seguir el conjunto de normas para cada dominio de la seguridad de la información por parte de los empleados de la Entidad, y terceros que presten servicios de información y tengan acceso a activos de información.

En su apartado 4.5.1.3, esta política establece:

*"**Responsabilidad por la seguridad de la información***

El cumplimiento de las políticas de seguridad de la información es obligatoria, esencial y legalmente requerida por POSITIVA Compañía de Seguros S.A., con el fin de tener una adecuada protección en sus activos de información.

Todos los funcionarios y terceros que laboran en POSITIVA Compañía de Seguros S.A. son responsables de cumplir las políticas de seguridad de la información establecidas en la Compañía.

Todas las descripciones de cargos deben contener detalles referentes a las responsabilidades específicas para el cumplimiento de las políticas de seguridad de la información en POSITIVA Compañía de Seguros S.A.

Los propietarios de la información de POSITIVA Compañía de Seguros S.A. deben asegurarse que los usuarios entiendan las condiciones y responsabilidades bajo las cuales se les ha brindado el acceso a la información y reconocer su deber de protegerla de cualquier amenaza de acuerdo a lo establecido en las políticas de seguridad de la información.

Esta política es norma general de cumplimiento dando alcance a las demás políticas enmarcadas en los dominios de la seguridad de la información.

b. Política de Organización de la Seguridad de la Información

Su objeto es dar pautas para gestionar la seguridad de la información de POSITIVA Compañía de Seguros S.A. como requisito de la Circular 042 de 2012 de la Superintendencia Financiera de Colombia, teniendo en cuenta lo siguiente:

•Compromiso con la seguridad de la información.
•Coordinación de seguridad de la información.
•Aplicación de responsabilidades de seguridad de la información.
•Proceso de autorización para instalaciones de procesamiento de información.
•Convenios de confidencialidad.
•Contacto con las autoridades.
•Contacto con los grupos de interés especial.
•Revisión independiente de la seguridad de la información.
•Identificación de los riesgos de tecnología de información relacionados con terceros.
•Enfocar la seguridad en el trato con los clientes y convenios con terceros.

El alcance de la política involucra los terceros con relación contractual con POSITIVA S.A. que tengan acceso a activos de información, y determina firmar acuerdos de confidencialidad para el manejo de estos.

Su apartado 4.1.2 define:

*" **Asignación de responsabilidades de seguridad de la información***

La asignación de responsabilidades se realiza conforme a los requerimientos de seguridad de la información (Ver Política de Seguridad de la Información). Protegiendo de esta manera los activos de la información.

El Propietario del activo de información puede delegar las tareas de seguridad; sin embargo, no lo exime de su responsabilidad, teniendo la obligación de supervisar y determinar el cumplimiento de las tareas delegadas con los requerimientos de seguridad. Las responsabilidades en las áreas serán definidas así:

· Identificar claramente los activos de información y procesos de seguridad asociados a este.
· El área responsable de cada activo de información o proceso de seguridad será notificada de esta responsabilidad, las cuales deben estar descritas en un documento.
· Los niveles de autorización deben estar claramente definidos y documentados.

(Ver Política de control de acceso de TI y Política de organización de seguridad de la información.)"

Con lo anterior, el acceso de terceros a los activos de información de POSITIVA S.A. debe estar debidamente regulado por los acuerdos de confidencialidad, y acorde al inventario de activos de información se debe catalogar la información que estos van a manejar en el proceso corporativo objeto de su contrato, y de esta forma efectuar el debido control.

El apartado 4.2 define:

· El personal que tiene acceso a los activos de información incluidos por cualquier contrato con POSITIVA Compañía de Seguros S.A. deberá acatar las políticas de Seguridad de la Información. El Comité Ejecutivo de Seguridad de la Información será el único que aprobará, en caso de requerirse, excepciones al cumplimiento de esta normatividad.
· Cualquier falta a las Políticas de Seguridad de la Información, por parte de un agente externo incluidos por contratos con POSITIVA Compañía de Seguros S.A., estará sujeta a las sanciones administrativas establecidas en el ANS (Acuerdo de Niveles de Servicio) y a las sanciones penales y civiles a que haya lugar.

Finalmente esta política define la necesidad de establecer claramente en la relación contractual los aspectos de control del tercero frente al acceso a la información de POSITIVA. El numeral 4.2.4 establece:

Acceso por terceras partes

El acceso de funcionarios contratados por terceras partes relacionados contractualmente con POSITIVA Compañía de Seguros S.A. representa un riesgo tanto en los aspectos físicos, como en los lógicos. Se deben tener en cuenta los siguientes aspectos:

· Acceso físico a oficinas, centros de cómputo, sitios de almacenamiento de información y otros sitios donde se encuentren recursos tecnológicos de POSITIVA Compañía de Seguros S.A.
· Acceso lógico a bases de datos, sistemas de información o cualquier otro almacenamiento de datos actuales o históricos de POSITIVA Compañía de Seguros S.A.
· Acceso para el soporte de hardware o software o a las funcionalidades de bajo nivel de las aplicaciones o sistemas.
· Los asociados o participes en el contrato o convenio pueden solicitar acceso a fin de intercambiar información, acceder los sistemas de información o compartir bases de datos.
· Controlar y evaluar al personal de contrato temporal y que pueden aumentar las debilidades de la seguridad de la información, como:
- Personal de mantenimiento y soporte de hardware y software.
- Los servicios de soporte contratados externamente (Outsourcing), como limpieza, cafetería, vigilancia y otros con acceso a las áreas donde se administren recursos tecnológicos.
- Los estudiantes en práctica.
- Los consultores.
· Identificar qué medidas de control se necesitan para administrar el acceso de terceras partes a los recursos tecnológicos y de procesamiento de información de POSITIVA Compañía de Seguros S.A..Todos los contratos con terceras partes deben reflejar todos los requisitos de seguridad de la información y controles internos que requiera el acceso de sus funcionarios.
· El acceso a terceras partes a los activos de información de POSITIVA Compañía de Seguros S.A., será autorizado con la firma del contrato, en donde están establecidas las medidas apropiadas de control.

Estándares asociados a esta política

1. Estándar de acuerdos de Nivel de Servicio

Aplica directamente a Contratos con terceros y su título 4.1 contiene definiciones para realizar los acuerdos de servicio, así:

4.1 DEFINICIONES PARA ACUERDOS DE SERVICIO.

Todos los Acuerdos de Nivel de Servicio relacionados con la seguridad de la información de POSITIVA Compañía de Seguros S.A. deben contener una serie mínima de asuntos predefinidos:

- *Servicios críticos que incluye.*
- *Usuarios y clientes de los servicios.*
- *Elementos de soporte necesarios para prestar el servicio.*
- *Aceptación de controles mínimos de seguridad.*
- *Expectativas de negocio respecto del rendimiento y la disponibilidad del servicio.*
- *Horario operativo para los servicios.*
- *Nivel de riesgo de negocio que no debe alcanzar el Acuerdo de Nivel de Servicio.*
- *Procedimientos de escalado.*
- *Tiempos de respuesta.*
- *Informes.*

En cuanto a los controles que se deben tener para garantizar el cumplimiento, se encuentran:

Los servicios, informes y controles deben monitorizarse y revisarse regularmente por parte de POSITIVA Compañía de Seguros S.A. y realizarse revisiones y auditorías periódicas.

El Acuerdo de Nivel de Servicio debe incluir el ámbito y periodicidad de los informes y auditorías.

Otros aspectos importantes a tener en cuenta en la inclusión y gestion de acuerdos de servicio son:

"…puede necesitar definirse y celebrarse periódicamente un comité de seguridad independiente, esto debe quedar plasmado dentro del acuerdo. Este comité se ocupará únicamente de asuntos, solicitudes y cumplimiento de seguridad."

"POSITIVA Compañía de Seguros S.A. mantendrá suficiente control global y conocimiento de todos los aspectos de seguridad respecto de la información confidencial y sobre las instalaciones a las que los terceros acceden o usan para procesar dicha información."

2. Estándar de Contratación con terceros

El presente estándar aplica en relación a todos los aspectos de seguridad de la información que define la Circular 042 de 2012 en lo concerniente a los terceros que presten servicios de procesamiento de datos y desarrollo de software con la entidad.

Los puntos a tener en cuenta son:

- CONFIDENCIALIDAD Y PROPIEDAD DE LA INFORMACIÓN
- RESTRICCIONES SOBRE EL SOFTWARE EMPLEADO
- NORMAS DE SEGURIDAD INFORMATICA Y FISÍCAS A SER APLICADAS
- IDENTIFICACIÓN DE PERSONAL QUE DEPENDE DEL CONTRATISTA

- PROCEDIMIENTO Y CONTROLES PARA LA ENTREGA DE LA INFORMACIÓN MANEJADA Y LA DESTRUCCIÓN DE LA MISMA
- PLANES DE CONTINGENCIA Y CONTINUIDAD DEL SERVICIO

3. Estándar de requerimientos de seguridad con terceros

Implica todos los aspectos de seguridad de la información que se deben incluir dentro de los contratos de prestación de servicios con terceros.

Se definen los tipos de terceros:

1. Terceros que acceden a los datos de POSITIVA Compañía de Seguros S.A. desde ubicaciones externas: cuando los datos residen en las máquinas de POSITIVA Compañía de Seguros S.A.
2. Terceros encargados de administrar datos de POSITIVA Compañía de Seguros S.A.: cuando los datos están ubicados y almacenados en las instalaciones de terceros.
3. Desarrollo y mantenimiento de software.
4. Tareas de gestión de la seguridad en la información.

Se define la Gestión y Análisis de Riesgos:

a) Las instalaciones de proceso de datos a las que los terceros han de acceder.

b) El tipo de acceso que tendrán a la información e instalaciones, como:
Acceso físico, es decir, a oficinas, salas de ordenadores, archivos.
Acceso lógico, es decir, a bases de datos, sistemas de información.
Conexiones de red entre la empresa y el tercero, es decir, conexión permanente, acceso remoto.
Si el acceso se hace on-site o desde fuera del sitio.

c) El valor y sensibilidad de la información afectada y la criticidad de las operaciones de negocio.

d) Los controles necesarios para proteger información que no ha de estar accesible para terceros.

e) El personal de la empresa del tercero encargado de gestionar la información.

f) Cómo se identifica a las empresas o personal autorizado a acceder, cómo se verifica la autorización y cada cuánto tiempo debe reconfirmase, así como de informar los cambios de personal para su debida autorización y seguimiento.

g) Los distintos medios y controles empleados por el tercero para almacenar, procesar, comunicar, compartir e intercambiar información.

h) El impacto que pueda producirse en caso de que el tercero no pueda acceder a la información cuando sea necesario y que ésta reciba información inadecuada o errónea.

i) Práctica y procedimientos para gestionar incidentes de seguridad de la información y daños potenciales y términos y condiciones para la continuidad del acceso de terceros en caso de incidentes de este tipo.

j) Requerimientos legales y otras obligaciones contractuales relevantes para el tercero que hayan de tenerse en cuenta.

k) Cómo los intereses de otros partícipes puedan verse afectados por los acuerdos.

Las cláusulas obligatorias que deben quedar en el contrato son:

- *Controles acordados a partir del análisis de riesgo.*
- *Política de seguridad en la información y normativas corporativas o locales.*
- *Controles y mecanismos de protección física.*
- *Norma de control de accesos, que incluya un proceso de autorización y asignación de privilegios a usuarios.*
- *Acuerdos sobre informes, notificación e investigación de incidentes y fallos de seguridad informáticos, así como de violaciones de los requisitos establecidos en el acuerdo.*
- *Derecho a auditar las responsabilidades definidas en el acuerdo, a que las mismas las realice un tercero y enumeración de los derechos establecidos para los auditores.*
- *Acuerdo de nivel de servicio, que cumpla con el documento VA-OD-EANS-01 Estándar para Acuerdos de Nivel de Servicio.*
- *Descripción del producto o servicio que se ofrece, así como una descripción de la información que debe estar disponible, junto con su clasificación de seguridad.*
- *El nivel de servicio objetivo y niveles de servicio inaceptables.*

Con respecto al acceso remoto a los sistemas de información de POSITIVA, se deben tener en cuenta las cláusulas:

a) Procedimientos restrictivos de administración de usuarios para asegurarse de que los nuevos usuarios y los borrados se realizan lo antes posible.

b) Una seguridad física adecuada para las instalaciones, salas de servidores y estaciones de trabajo que conectan remotamente con POSITIVA Compañía de Seguros S.A.

c) Restricciones de copia y difusión de información y uso de acuerdos de confidencialidad.

d) Políticas de control de acceso, que incluyan:

- *Las distintas razones, requerimientos y beneficios que hagan necesario el acceso del tercero.*
- *Métodos de acceso permitidos, así como el control y uso de identificadores únicos como usuarios y contraseñas.*
- *Requerimiento de mantener disponible una lista de personas autorizadas a utilizar los servicios y cuáles son sus privilegios y derechos a este respecto.*
- *Todo acceso no autorizado explícitamente está prohibido.*
- *Proceso de revocación de derechos de acceso o de interrupción de conexiones entre sistemas.*

Con respecto a los contratos con terceros para desarrollo y mantenimiento de Software, se deben incluir las siguientes claúsulas:

a) Acuerdos de licencia, propiedad del código y derechos de propiedad intelectual.
b) Certificación de la calidad y adecuación de trabajo realizado.
c) Acuerdos de escrow en caso de incumplimiento del tercero.
d) Derechos de acceso a auditar la calidad y adecuación de trabajo realizado.
e) Requisitos contractuales respecto de la calidad y funcionalidad en seguridad del código.
f) Pruebas antes de la instalación para detectar código malicioso o troyanos

c. Política de Seguridad Física y Ambiental

Esta política implica el mantener control de acceso a las sedes y a la información de POSITIVA S.A., en lo que respecta al perímetro físico y sus controles de acceso, mantenimiento de áreas seguras, el acceso público, áreas de carga y descarga y protección de equipos, entre otras disposiciones.

En su apartado 3.1 la política expresa:

"Todo acceso de los funcionarios, terceros (proveedores o contratistas) y afiliados que por razones inherentes a su vínculo con POSITIVA Compañía de Seguros S.A. requieran utilizar las instalaciones y los sistemas de información, debe ser debidamente autorizado, monitoreado."

El apartado 4.3 indica:

"Todos los empleados y terceros (contratistas, proveedores) que tengan acceso a las áreas de POSITIVA Compañía de Seguros S.A. donde se procesa información, son responsables por el buen funcionamiento y estado de los sistemas de información e instalaciones."

El apartado 4.7 establece:

"· Los empleados y terceros (proveedores y contratistas) que mantienen una relación contractual con POSITIVA Compañía de Seguros S.A., sólo podrán acceder las áreas de la Compañía que procesan, almacenan o transmiten información cuando sea requerido. Este acceso debe ser planeado, autorizado y supervisado.
· No se permite el ingreso de dispositivos"

El capítulo 7 CUMPLIMIENTO DE LA POLÍTICA SEGURIDAD FISICA Y AMBIENTAL expresa en relación al incumplimiento por parte de terceros:

"En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia)."

d. Estándares asociados a esta política

1. Estándar de Seguridad de los Equipos

Este estándar dicta normas en la seguridad en el uso de equipos de cómputo asignados a funcionarios y terceros.

El estándar puntualmente define:

"Los equipos que sean propiedad o estén bajo custodia de POSITIVA Compañía de Seguros S.A. deben contar con la protección y seguridad apropiada para reducir los riesgos provenientes de amenazas físicas, ambientales y humanas.

Todas las áreas e instalaciones de POSITIVA Compañía de Seguros S.A., que contengan o realicen procesamiento de información deben contar con controles adecuados para evitar el acceso físico no autorizado, el daño o interferencia a la información de la organización."

Con respecto a equipos de terceros y en lo relacionado con soporte y mantenimiento, la norma específica que esta labor debe ser proporcionada por el tercero contratado:

"Se debe contar con un adecuado soporte técnico, respaldado por contratos con garantía de provisión o sustitución temporal del equipo, o de uno o varios de sus componentes en caso de falla, daño o hurto."

Con respecto a equipos que se encuentren fuera de instalaciones de POSITIVA, el estándar indica:

"Los equipos y los medios de información o almacenamiento que se encuentran fuera de las instalaciones de POSITIVA Compañía de Seguros S.A no se deberían dejar solos en sitios públicos..."

Se deben determinar los controles apropiados con base en los riesgos evaluados para el trabajo desde casa o desde sitios externos a POSITIVA Compañía de Seguros, para controlar el acceso a las redes o información.

Los equipos que se encuentren fuera de las instalaciones de POSITIVA Compañía de Seguros S.A. deberían proteger la información almacena con software que permita el cifrado de discos y el acceso por contraseña, para evitar la pérdida de confidencial de la información.

2. Estándar para el control de Acceso Físico

Este estándar pretende mantener unas reglas específicas para controlar el acceso por parte de tereceros a las instalaciones de POSITIVA.

Con respecto al ingreso de eerceros y visitantes, el estándar especifica:

- *El ingreso a las áreas de POSITIVA Compañía de Seguros S.A., debe ser aprobado por un funcionario de la Compañía, quien será el responsable del visitante mientras permanezca en las instalaciones de POSITIVA Compañía de Seguros S.A.*
- *Todos los visitantes, sin excepción alguna deben identificarse y registrarse en el área de recepción de POSITIVA Compañía de Seguros S.A.*
- *Todo el personal de terceros contratados para ejecutar o realizar tareas dentro de las instalaciones, recintos u oficinas de POSITIVA Compañía de Seguros deben ser identificados como visitantes y deben cumplir con los controles de acceso físico e identificación establecidos.*
- *Todo visitante debe portar una identificación visible, con su respectiva tarjeta de aproximación que le permitirá dirigirse únicamente al piso donde está ubicada la persona que va a visitar, y una ficha que debe ser firmada por el funcionario quien recibió la visita y será entregada en la recepción al momento de la salida de las instalaciones de POSITIVA Compañía de Seguros S.A. previo reclamo de su documento que dejo al ingresar.*
- *Los visitantes que se encuentren sin acompañamiento ó cualquiera que no lleve identificación visible, deben ser evacuados de dichas áreas y reportar al área de seguridad.*
- *Es responsabilidad de los funcionarios visitados, verificar que los dispositivos que los visitantes porten con ellos a POSITIVA Compañía de Seguros S.A., no lleven información del mismo.*
- *Se debe restringir el acceso a las áreas sensibles por parte del personal, de los proveedores o de mantenimiento, solo a los casos en que sea requerido y autorizado. Aun con acceso autorizado, se debe registrar el acceso y se deben controlar sus actividades por parte del funcionario visitado (especialmente en zonas de datos sensibles).*

- *Se deben cumplir las políticas y estándares en referencia a la salida y entrada física de soportes de información (impresos,*

- *El acceso físico a áreas restringidas debe ser controlado. Visitantes y personal de servicio que no esté autorizado a entrar regularmente, deben ir acompañados por la persona responsable de su visita. El personal con autorización a entrar en las áreas restringidas debe ser informado por el administrador del área de los riesgos de seguridad implícitos.*

3. Estándar de instalación y desinstalación de software y hardware

Este estándar contempla parámetros para instalar y desinstalar software y hardware requerido por funcionarios y terceros para ejercer labores dentro o fuera de la entidad.

Con respecto a la instalación de Hardware, el estándar indica:

"Los funcionarios responsables de la infraestructura tecnológica (eléctrica, computacional y de comunicaciones), deben realizar la revisión de los diferentes equipos, dispositivos y recursos para efectos de detectar averías, defectos o alteraciones, y de tal forma garantizar su protección y su adecuado funcionamiento."

La instalación de elementos de hardware y de software será autorizada solo por personal autorizado de la Gerencia de Infraestructura de la Entidad.
La norma dispone las frecuencias de revisión y el formato de reportes que garanticen el cumplimiento de este estándar por parte de funcionarios y terceros.

e. Política de Cumplimiento de requisitos legales en TI

Esta política está relacionada con la regulación nacional vigente en lo que respecta a la seguridad de la información y protección de datos personales. Su cumplimiento aplica a todos los funcionarios y terceros en relación contractual con POSITIVA S.A.

Se debe tener control de temas como: derecho a la propiedad intelectual, licenciamiento para el uso de software, y protección de datos personales de empleados, terceros y clientes, así como velar por que los terceros protejan la información de carácter personal de clientes o funcionarios que le sea entregada para su procesamiento, dentro del objeto contratual.

Estándares asociados a esta política

1. Estándar de Contratación con terceros

Este estándar ya fue analizado en la política de Organización de la Seguridad

2. Estándar de Requisitos legales y normativos

Su propósito es identificar oportunamente la normatividad aplicable y desarrollar las actividades necesarias implementando las medidas y controles necesarios para satisfacer adecuadamente los requisitos exigidos.

La actualización de los listados normativos a cumplir por POSITIVA S.A. estará en cabeza de la Oficina Asesora Jurídica, siendo también labor de la Vice TIC, observar y actualizar lo concerniente en cuanro a legislación en materia tecnológica.

Este estándar es aplicable a terceros en virtud del vínculo contractual y en razón a los acuerdos de confidencialidad y los acuerdos de niveles de servicio. Las normas que debe cumplir POSITIVA, son extensivas a los prestadores de Servicios.

Se deben ejercer los controles adecuados con funcionarios y terceros para garantizar estos cumplimientos, siendo las auditorias periódicas, el método primario para ejercer dicho control.

f. Política de Gestión de Activos de Información

Esta política busca el entendimiento, de funcionarios y terceros con relación contractual con POSITIVA S.A., de las responsabilidades y actividades en pro de la protección de los activos de Información inventariados a su cargo, catalogados en:

- Hardware.
- Software.
- Procesos y procedimientos.
- Personas.
- Información.
- Intangibles

La clasificación de la información en POSITIVA S.A. está dada por:

"Toda la información de POSITIVA Compañía de Seguros S.A. es clasificada en los siguientes niveles: interna, pública y confidencial."

"Toda información que no ha sido clasificada o etiquetada, será tratada como publica."

El numeral 4.6 Difusión a los usuarios de la información, establece:

"Una vez clasificada la información es necesario realizar un proceso de socialización para que los usuarios conozcan cuales son los datos críticos y la información propia de su área que requiere un mayor nivel de protección. Este proceso de socialización y concientización se llevará a:

· Funcionarios de POSITIVA Compañía de Seguros S.A.
· Terceros y personal temporal contratado."

Con respecto al cumplimiento por parte de terceros, el numeral 7 indica:

"*En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia)."*

Estándares asociados a esta política

1. Estándar de Etiquetado de Información

Esta norma indica la necesidad de llevar un control de la información clasificada como confidencial, por medio de una etiqueta que colocará el dueño del activo, donde indique el carácter confidencial de estos activos. Los terceros prestadores de servicios, por medio de la relación contractual y de los acuerdos de confidencialidad pactados, se deben hacer

responsables del manejo adecuado de activos confidenciales otorgados en custodia por POSITIVA, en razón al servicio contratado.

g. Política de Adquisición, desarrollo y mantenimiento de Sistemas.

El alcance de esta política está definido por:

"La Política de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información en POSITIVA Compañía de Seguros S.A. involucra directamente a todo personal interno ó externo de POSITIVA Compañía de Seguros S.A., que realice funciones o tenga responsabilidades en los procesos de adquisición, desarrollo y mantenimiento de sistemas de información."

Esta política define las normas a ser cumplidas por funcionarios y terceros (proveedores y contratistas) de POSITIVA Compañía de Seguros S.A. sobre las funciones, planes y responsabilidades para la adquisición, desarrollo y mantenimiento de sistemas de Información que tiene como objetivo la definición de un marco de referencia que responda a los objetivos estratégicos de la organización.

Estándares asociados a esta política

1. **Estándar de control de versiones de Software**

   Este estándar contiene la normativa para el manejo y control de versiones de Software entregadas por terceros, para lo cual POSITIVA en cabeza de la Vicepresidencia de TIC, proveerá la plataforma adecuada para llevar la documentación respectiva.

   Dado que el proceso asociado a desarrollo de software es de manejo tercerizado en virtud de contratos de prestación de servicios, todos los prestadores deben acogerse a este estándar como buena práctica de trabajo.

2. **Estándar de control de cambios en SI**

   Este estándar indica los lineamientos que se deben cumplir al requerirse cambios de configuración en los sistemas de información en virtud de nuevos requerimientos o cambios en las versiones del Software. El estándar indica los niveles clasificados de cambios (estándar, significativo, mayor, de Emergencia), y la prioridad que deben llevar cada uno de ellos.

   Dado que el proceso asociado a desarrollo de software y mantenimiento de sistemas de información es de manejo tercerizado en virtud de contratos de prestación de servicios, todos los prestadores deben acogerse a este estándar como buena práctica de trabajo. De igual manera, el estándar indica la creación del **comité de control de cambios**, dentro del cual debe haber integrantes técnicos de parte del tercero.

3. **Estándar de enmascaramiento de datos**

   Indica la necesidad de generar cambios en los campos considerados confidenciales, en la información extraída de las bases de datos misionales, y que sería entregada a funcionarios y terceros para efectos de desarrollo y pruebas de sistemas de información. Esta norma es de cumplimiento estricto de parte de POSITIVA frente a los terceros, en razón a la vigilancia de la norma 042 de la SFC y de la Ley 1581 de 2012.

4. Estándar de Ejecución de Proyectos

Indica las pautas a seguir en la formulación y seguimiento de proyectos por parte de POSITIVA hacia los terceros proveedores de servicio. Allí se dictan las fases claras del proyecto y los entregables de cada una.

5. Estándar de gestión de configuración

Indica los elementos a tener en cuenta en la parametrización, las líneas base de entrega y los controles de cambios aplicables a sistemas de información dentro de la entidad.

El objetivo de la gestión de la configuración es mantener la integridad de los productos que se obtienen a lo largo del desarrollo de los sistemas de información, garantizando que los cambios son controlados y que todos los participantes en el desarrollo de sistemas ó aplicaciones disponen de la versión adecuada de los productos que manejan.

En este estándar se señalan los elementos a contemplar como parte del control por parte de POSITIVA con los terceros prestadores de servicio, en la verificación y auditoria de la configuración de los Sistemas de Información, y en los contenidos de los informes que de esta gestión se realicen.

6. Estándar de Gestión de Vulnerabilidades Técnicas

La norma indica la necesidad de realizar al menos dos (2) veces por año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación de POSITIVA Compañía de Seguros S.A. que usen internet como canal para sus operaciones. Si se realizan cambios en los sistemas que afecten la seguridad del canal se deben realizar pruebas adicionales.

El estándar indica los requerimientos de las pruebas de penetración y vulnerabilidad que se deben realizar, y del contenido de los informes que se deben documentar. Se debe dejar clara la responsabilidad de los terceros en la remediación de las brechas encontradas dentro de los sistemas de información desarrollados por estos, por medio de la relación contractual en los acuerdos de nivel de servicios.

7. Estándar de implantación y aceptación de sistemas

Este estándar tiene como objetivo principal la entrega y aceptación de cualquier sistema para POSITIVA Compañía de Seguros S.A. y la realización de todas las actividades necesarias para el paso a producción del mismo. Se define un plan de implantación y se especifica el equipo que lo va a llevar a cabo en POSITIVA Compañía de Seguros S.A.

Este documento es de cumplimiento obligatorio por parte de los terceros prestadores de servicios, por ser un compendio de pasos a seguir en la salida a producción de cualquier sistema de información entregado.

8. Estándar de Migración de Datos

Este estándar involucra directamente al personal de la Gerencia de Soluciones de TI o personal externo de POSITIVA Compañía de Seguros S.A., que tenga acceso a los sistemas, bases de datos y aplicaciones que manejen información de la compañía que deseen ser migrados o trasladados a nuevos ambientes.

En este documento se especifican los pasos a seguir, la documentación y el control que se debe llevar en procesos de migración de datos, para la entrega a procesos internos o

ejecutados por terceros, y que son de estricto y obligatorio cumplimiento por parte de funcionarios y prestadores del servicio.

Uno de los aspectos a tener en cuenta es los controles de gestión y operacionales de seguridad. Dentro de los controles se debe observar:

- Personal de seguridad
- Protección física y ambiental
- Controles en producción
- Planes de contingencia.
- Sistemas de control de hardware
- Controles de mantenimiento de software
- Integridad de datos/ controles de validación
- Reporte de incidentes
- Cifrado de datos

9. Estándar de seguridad de los sistemas de Información

Este documento contiene normativas para mantener la seguridad en los sistemas de información de POSITIVA, por parte de funcionarios y terceros involucrados en su manejo.

La norma indica las fases procedimentales para proveer seguridad en un sistema de información, así como la normatividad que se debe cumplir a nivel de estándares, leyes o regulaciones. Se debe hacer un análisis minucioso de los requerimiento de seguridad del sistema de información, y hacerlos exigibles al proveedor del mismo. Los requisitos a considerar son:

- *Mecanismos de seguridad que proporcionan los sistemas.*
- *Confidencialidad, integridad y disponibilidad de la información, establecido por el departamento o área que operará el sistema con la ayuda de la Gerencia informática.*
- *Tipo de datos a proteger.*
    - *Datos de carácter personal.*
    - *Datos relacionados con la actividad de la organización, clientes, bancaria, personal que desde el punto de vista del negocio puedan afectar a la imagen del grupo o a la relación con los clientes.*
- *Flujos de información internos y externos.*
- *Protocolos de redes usados*
- *Arquitectura de autenticación*
- *Necesidad de usar criptografía en las aplicaciones*
- *Segregación de entornos*
- *Registros de auditoria*
- *Gestión de los catálogos de contenidos (publicación, lista de los contenidos y transacciones disponibles a cada tipo de usuario etc.)*
- *Políticas de seguridad de POSITIVA Compañía de seguros S.A.*
- *Necesidad de cumplir los estándares del sector y los procesos de certificación.*
- *Planes de contingencia y de disponibilidad*

Durante la fase de requisitos se debe realizar:

- *El inventario de los componentes implicados y requeridos, tanto para las diferentes fases del ciclo de vida de desarrollo del sistema o aplicación como lo que se requiere para garantizar la seguridad global de la aplicación y su entorno durantecada fase del ciclo de vida.*

    - *Componentes de la arquitectura*
    - *Componentes de hardware*
    - *Lenguajes de programación*
    - *Entorno de desarrollo*

- *Entorno de producción*
- *Herramientas de depuración*

- *La descripción del tipo de información manejada, y la posible normativa legal que le aplique:*
  - *Modelo de datos (requisito general de Ingeniería del Software)*
- *Asociado a lo anterior: clasificación de la información*
- *Requisitos legales y regulatorios aplicables*
- *Descripción de la parte operativa del servicio (tipología de usuarios, segregación de funciones, canales de acceso etc.)*

Una vez surtidas todas las consideraciones de seguridad en las fases del proyecto, y este puesto en producción, se deben realizar las pruebas periódicas de análisis de vulnerabilidad, que en caso de arrojar como resultado brechas, deben ser pasadas al proveedor del servicio para remediación en virtud de contratos de mantenimiento del sistema de información.

Otros temas a tener en cuenta en la validación de seguridad en sistemas de información son:

- Seguridad en las redes y canales de acceso
- Protección contra malware y códigos maliciosos
- Auditoria y trazabilidad
- Documentación de las excepciones de seguridad

h. Política de Gestión de Comunicaciones y Operaciones

Aplica a la operación de los sistemas de información, el control de cambios y los riesgos asociados a su administración. Debe ser cumplida por todos los funcionarios y terceros con vínculo contractual que manejen cualquier tipo de información de POSITIVA S.A.

Dentro de las generalidades de aplicación, la política indica:

"Todos los funcionarios y terceros (proveedores y contratistas) que realicen actividades de desarrollo y administración de activos en los sistemas de información de POSITIVA Compañía de Seguros S.A., deben implementar un procedimiento formal al momento de realizar un cambio en las tecnologías de información."

En el apartado sobre "seguridad en los servicios de red" se determina la necesidad de monitorear la capacidad de los proveedores de servicio, acordando las auditorias requeridas. Se deben establecer acuerdos de servicio, requerimientos de gestión y niveles de seguridad de la información, asegurándose de verificar que se implementen todas estas medidas.

El apartado 4.81 sobre gestión de medios de almacenamiento indica:

"El supervisor de la contratación de servicios de procesamiento de información por parte de POSITIVA Compañía de Seguros S.A., deberá seleccionar adecuadamente el contratista, acorde a su experiencia, buen nombre y la calidad de sus controles, en suma con las condiciones exigidas por la necesidad del contrato y los niveles de acuerdo de servicio pactados, para garantizar el manejo idóneo de la información como activo de propiedad de POSITIVA Compañía de Seguros S.A."

En el apartado 7 sobre cumplimiento, se expresa con respecto a terceros, lo siguiente:

En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia).

Estándares asociados a esta política

1. Estándar de Administración de entrega de servicios a terceros

Este estándar contiene la normativa para mantener un grado adecuado de seguridad de los activos de información accedidos o procesados por terceros, de conformidad con los acuerdos de prestación del servicio por terceros contratados por POSITIVA.

La norma aplica a todos los empleados de POSITIVA Compañía de Seguros S.A. afectados en establecer acuerdos con terceros y a los mismos terceros afectados que tengan acceso a los sistemas y activos de información pertenecientes a POSITIVA.

La prestación de servicios por terceros debe incluir:

- *Los acuerdos sobre disposiciones de seguridad.*
- *Definiciones del servicio.*
- *Aspectos de la gestión del mismo.*

Debe haber un contrato legal para asegurar que los terceros adoptan los controles relevantes de seguridad de la información descritos en el manual de políticas de seguridad de la información de POSITIVA.

El contrato es un documento legalmente vinculante que desde la perspectiva de seguridad tiene que incluir:

- *Adhesión y referencia a las norma de seguridad de la información.*
- *Las medidas de seguridad.*
- *Acuerdos de no divulgación.*
- *Acuerdos financieros relacionados con el servicio.*
- *Procedimientos de gestión en caso de interrupción o fallo en el servicio.*
- *Derecho de la unidad de revisar el proceso y los dispositivos de seguridad.*
- *Relaciones del tercero con subcontratas y otros participantes.*
- *Límites de responsabilidad de terceros.*
- *Procedimientos de rescisión que incluyan devolución de activos.*

En cuanto a acuerdos de confidencialidad, la norma expresa:

Las compañías que actúen como terceros tienen la responsabilidad de asegurar que todo su personal que aceda a activos de información de POSITIVA Compañía de Seguros S.A. conozca sus responsabilidades, todo personal de terceros debe firmar un acuerdo de confidencialidad. Este establecerá claramente a que activos de información puede acceder y que mecanismos de seguridad tienen que cumplir.

La norma también define la necesidad de establecer una evaluación de la seguridad del tercero frente a los servicios que presta, en lo que respecta a:

"…la capacidad del tercero en instalaciones y procesos de operación y que ofrece un nivel de seguridad adecuado. Debe evaluarse el riesgo de contar con un tercero e identificarse los requisitos de seguridad antes de pueda comenzar el contrato."

Cuando el producto sea software terminado, se debe tener en cuenta lo siguiente: *"…El tercero debe establecer y garantizar la calidad del software que desarrolla o emplea para dar soporte a procesos del negocio, así como que es capaz de ofrecer niveles adecuados de soporte y mantenimiento de acuerdo a los niveles de servicio estipulados."*

La norma incluye la necesidad de controlar acceso remoto de los terceros a los Sistemas de Información de POSITIVA, dejando documentada la necesidad por requerimientos del servicio.

Se exige también el monitoreo y supervisión continua de las actividades de los terceros en los Sistemas de Información de la Entidad.

2. Estándar de control de cambios en sistemas de información

Ya este estándar fue revisado dentro de la política de Adquisición desarrollo y mantenimiento de sistemas

3. Estándar para controles de red

Este estándar contiene la normativa requerida para tener controles de acceso a la red y disgregar las conexiones de Funcionarios, Terceros y Visitantes, dentro de las instalaciones de POSITIVA S.A., con niveles de acceso bien definidos y en lo posible separados para diferenciar el tráfico de cada red.

Sugiere un conjunto de capas que definen los servicios a que tiene derecho un determinado usuario. Estas capas se deben plasmar en “planos de seguridad” que sirven para plasmar la seguridad implementada en un esquema de fácil lectura a quien ejerce los controles.

El objetivo final de este estándar es garantizar el cumplimiento de los objetivos de seguridad, en razón a:

- Control del acceso
- Autenticación
- No-repudio
- Confidencialidad de los datos
- Seguridad del flujo de comunicación
- Integridad de los datos
- Disponibilidad
- Privacidad

4. Estándar de control de versiones de Software

Ya analizado en la política de Adquisición, desarrollo y mantenimiento de Sistemas.

5. Estándar de gestión de configuración

Ya analizado en la política de Adquisición, desarrollo y mantenimiento de Sistemas.

6. Estándar de implantación y aceptación de sistemas

Ya analizado en la política de Adquisición, desarrollo y mantenimiento de Sistemas.

7. Estándar para el Manejo de Medios de la Información e Intercambio de Información

Este estándar es una guía de manejo para medios de almacenamiento dentro de POSITIVA S.A., tanto por parte de Funcionarios, como de terceros asociados a procesos de información de la entidad.

Establece las normas para la toma y resguardo de copias de seguridad para los sistemas misionales, y para el manejo de intercambios de información entre funcionarios, y entre funcionarios y terceros, a través del manejo de formatos específicos para la documentación de estos procedimientos.

Dentro de la documentación se debe tener en cuenta la clasificación dada a la información y los responsables de su manejo. Los criterios a tener en cuenta son:

- Responsables de la información
- Uso de la información
- Identificación de la información
- Valor de la información
- Edad de la información
- Nivel de daño
- Nivel de protección
- Nivel de responsabilidad

El control de los medios inicia en la marcación o etiquetado del dispositivo físico de almacenamiento, el cual debe contener datos como:

- Nombre del archivo o archivos contenidos
- Identificación del archivo o archivos (archivo maestro, base de datos, archivo primario, archivo temporal, entre otros).
- Tamaño del archivo.
- Identificación del sistema o aplicación que usa el archivo o archivos y/o permite su administración.
- Formato de compresión y/o empaquetamiento [si el archivo (o archivos) presenta dicha característica].
- Versión del archivo o archivos (si existe).
- Fecha de última actualización.
- Fecha de almacenamiento.

Otros aspectos que considera el estándar a ser tenidos en cuenta son: la localización, la ubicación, la forma de almacenamiento y conservación de los medios, el transporte y la destrucción de los medios.

8. Estándar para la Protección contra software malicioso y códigos móviles.

El estándar define la necesidad de contar con software de protección contra software malicioso, y virus o gusanos que afectan el rendimiento del sistema y abren brechas que permiten la pérdida de información. Se debe instalar el control en todas las máquinas de la entidad y para el caso de terceros que requieren conexión a la red de la entidad, se debe realizar una revisión previa para verificar la existencia actualizada de este tipo de software antes de conectarla.

También hace énfasis en el control de acceso a internet a funcionarios y terceros, para que se garantice una navegación “limpia”, sin acceso a sitios maliciosos o que contengan software atacante, por medio de un filtrado web fuerte.

El incumplimiento de este estándar por parte de funcionarios o terceros, conlleva graves riesgos de seguridad, por tanto se hace obligatorio el efectuar control, haciendo énfasis en las maquinas que visitantes o terceros requieren conectar a la red de la entidad.

i. Política de Control de Acceso de TI

El objetivo de esta política es mantener el control de acceso a la información en POSITIVA S.A. acorde a lo establecido en la circular 042 de 2012 de la SFC.

El alcance indica que la aplicación de la política corresponde a:

Se hace referencia al acceso físico de los usuarios internos y externos a los activos de los sistemas de información cuando se autoriza acceso a las áreas donde se procese información o funcionen sistemas de información con datos sensibles, restringidos o confidenciales, como:

- *Áreas de transmisión de información de casa matriz o en regionales.*
- *Áreas de tesorería o de manejo de información especial (depósitos judiciales).*
- *Áreas de almacenamiento de información magnética o documental.*
- *Áreas de comunicaciones.*
- *Áreas de administración de control de acceso, Internet y correo electrónico.*
- *Las edificaciones de las diferentes sedes o regionales donde se encuentra ubicado cualquier tipo de activo (hardware, software, información, personas, procesos, entre otros) que hacen parte de los sistemas de información.*
- *Los centros de cómputo donde se encuentran ubicados cualquiera de los activos de información de los sistemas de información.*
- *Las salas de cómputo, oficinas, kioscos y cualquier infraestructura física que sea un lugar donde se encuentra ubicado cualquier tipo de activo de los sistemas de información.*

· Todos los usuarios internos y externos de POSITIVA Compañía de Seguros S.A. que se encuentran autorizados para acceder a los sistemas de información y cualquiera de sus aplicaciones. Se consideran:

- Usuarios externos: al personal que tenga algún vínculo o relación contractual para recibir un servicio o producto con POSITIVA Compañía de Seguros S.A. Dentro de éstos se encuentran los clientes. Igualmente, puede formar parte de los Usuarios externos cualquier tipo de persona externa a POSITIVA Compañía de Seguros S.A. que no tenga una relación contractual con la Compañía y que por alguna razón especial o excepción se le otorgue acceso a cualquier tipo de activo de los sistemas de información, por ejemplo: entes de control, autoridades civiles o militares.

El apartado 4.7 de esta política indica las responsabilidades de terceros en el manejo de claves de acceso a los sistemas de información:

Los funcionarios y terceros (proveedores y contratistas) que laboran en POSITIVA Compañía de Seguros S.A. tienen responsabilidad sobre los códigos de acceso asignados para los sistemas de información y siguen las recomendaciones del VA-OD-ECAL-03 Estándar Control de Acceso Lógico para la creación de contraseñas seguras.

La cooperación de los usuarios es esencial para la eficacia de la Seguridad de la Información de los sistemas de información, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el uso y ejecución de controles de acceso eficaces para los sistemas de información, en particular aquellos relacionados con el uso de claves y la seguridad de los equipos de cómputo y a la información.

Con respecto al cumplimiento de la política, el numeral 7 indica:

En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia).

Estándares asociados a esta política

1. Estándar de control de Acceso Lógico

Este estándar propone un marco de acción para la nomenclatura de creación de usuarios y las condiciones de asignación y restablecimiento de claves de acceso.

- *El nombre de Usuario de Red es el número de Cédula.*
- *El nombre de Usuario de Correo se usa el Nombre y Apellido en caso de ser Homónimos se usa el 2 apellido.*
- *Tamaño mínimo de la clave: seis (6) caracteres.*
- *Compuesta por: combinación que incluya números, letras (mayúsculas y minúsculas) y símbolos o caracteres especiales ($, %, &, *).*
- *La contraseña inicial emitida a un nuevo Usuario sólo es válida para la primera sesión. En ese momento, el Usuario debe escoger otra contraseña.*
- *Vigencia máxima: cada sesenta (60) días como máximo, el sistema solicitará el cambio de clave, la contraseña no debe ser igual a las últimas tres contraseñas utilizadas.*
- *Bloqueo por intentos: después de cinco (5) intentos fallidos, la cuenta se bloquea y el usuario debe alertar al Administrador del Sistema, si se trata de acceso remoto via modem por discado, la sesión debe ser inmediatamente desconectada.*
- *Las contraseñas predefinidas que traen los equipos*

Este documento define también los roles y tipos de usuarios sugeridos para el acceso a los sistemas de información, junto con una descripción de la función que ejerce cada uno. Cada usuario debe tener definido un rol asociado a su usuario.

j. Política de Gestión del Riesgo en TI

Esta política está encaminada a establecer una guía en el manejo y contextualización de los riesgos en los sistemas de información, definiendo el alcance del Sistema de Gestión del Riesgo, enfocado en el inventario de activos de información de la entidad.

El alcance implica cumplimiento por parte terceros en la observancia de los riesgos asociados a los activos de información y la mitigación que se debe hacer de estos:

El Sistema de Administración de Riesgo de tecnologías de la información en POSITIVA Compañía de Seguros S.A. involucra a:

· Todos los clientes y terceros, sobre los cuales recae la responsabilidad del cumplimiento de las políticas, normas y procedimientos de seguridad informática que se establezcan en POSITIVA Compañía de Seguros S.A.

La gestión del riesgo debe ser realizada en los activos Inventariados. La implementación del sistema de gestión de riesgos pretende evaluar los activos donde se encuentra la información en todo su proceso (generación, transporte, procesamiento y almacenamiento).

Mediante la gestión de riesgo de tecnologías de la información sobre el recurso humano, es importante considerar:

· El nivel de acceso y privilegios que tienen los usuarios de los sistemas de información, en lo que concierne a redes y sus aplicaciones, y a la parte física donde se encuentran ubicados los dispositivos que hacen parte de estos sistemas de información.
· La responsabilidad de los usuarios sobre cada uno de los activos que le han sido asignados y que hacen parte de los sistemas de información.
· La capacitación y formación educativa mínima requerida para acceder y manipular información.
· El nivel técnico del personal de la Vicepresidencia de TIC's que maneja la infraestructura de los sistemas de información de POSITIVA Compañía de Seguros S.A.

Con respecto al cumplimiento de la política, el numeral 7 indica:

En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia).

k. Política de Seguridad de la Información Frente al Recurso Humano

El objetivo de esta política es garantizar que funcionarios y terceros comprendan las responsabilidades implícitas en el manejo de activos de información de POSITIVA S.A.

Con respecto a los procesos de selección de personal, la política define:

…. todos los servidores públicos (Empleados Públicos y Trabadores Oficiales), y personal que preste sus servicios en forma tercerizada, pasantes practicantes y toda aquella persona que por relación contractual tenga acceso a los activos de información al iniciar sus labores y vínculo contractual con la Compañía serán conocedores de sus obligaciones, compromisos y las consecuencias del incumplimiento de la presente política. Para lo cual dentro del proceso de inducción se capacitará a los funcionarios y se les entregará el contenido de este documento. Una vez se realice lo anteriormente descrito cada persona firmará el formato de conocimiento y aceptación de la presente Política.

Las responsabilidades de los funcionarios y terceros en cumplimiento del manejo de los activos de la información son las siguientes:

· Actuar conforme a esta política contenida en el documento Política de Seguridad de la Información.
· Proteger los activos de información de acceso no autorizado evitando su modificación o destrucción, de acuerdo con los aspectos descritos en la Política de Control de Acceso de TI.
· Informar los incidentes de seguridad de la información de acuerdo a la Política de gestión de incidentes de SI, cuando los incidentes pueden comprometer los activos de información de POSITIVA Compañía de Seguros S.A.

Con respecto a los términos de la vinculación, se establece:

·Todo funcionario o tercero que de acuerdo al cargo que ejerza, acceda a un activo de información firmará una cláusula de confidencialidad (Ver documento Política de Organización de Seguridad de la Información).
· POSITIVA Compañía de Seguros S.A. le informará al funcionario la responsabilidad de clasificar la información a la cual acceda en el ejercicio de sus funciones de conformidad a la Política de Gestión de Activos de Información (Ver documento

Política de Gestión de Activos de Información).
· Responsabilidad para el manejo de la información personal de los candidatos.
· Responsabilidades que se extienden fuera del área física o del horario laboral de POSITIVA Compañía de Seguros S.A.

En el cumplimiento de las funciones, el funcionario o terceros deben observar:

La responsabilidad de POSITIVA Compañía de Seguros S.A. está en asegurar que sus funcionarios:

· Apliquen las normas generales descritas en las políticas de seguridad de la Información.
· Estén informados de sus deberes de seguridad de la información antes de acceder a la misma.
· Alcanzar un nivel de conocimiento y conciencia de seguridad de la Información frente a sus funciones y responsabilidades en la Compañía.
· Desarrollen métodos apropiados de trabajo para cumplimiento de las actividades de POSITIVA Compañía de Seguros S.A. sin poner en riesgo la integridad de la información.

En el apartado 4.3 sobre Terminación del empleo o traslado del cargo se indican medidas a tomar con respecto a la salida de funcionarios o terceros y la obligatoriedad de devolver los activos de información bajo su custodia y el retiro de permisos sobre los sistemas de información.

Con respecto al cumplimiento de la política, el numeral 7 indica:

En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia).

I. Política de Gestión de Incidentes de TI

Esta política tiene por objeto dimensionar los riesgos asociados a los activos tecnológicos, tener planes de acciones preventivas y correctivas oportunas, asegurando de esta forma las debilidades.

"… esta política aplica a los funcionarios y empleados de terceros que se encuentran vinculados con POSITIVA mediante deberes contractuales o fiduciarios, tácitos o explícitos, y mientras registren, utilicen o mantengan en custodia los recursos de información y los recursos informáticos de POSITIVA."

Con respecto a las Normas generales, relacionadas con terceros, la norma expresa:

Todos los funcionarios, terceros y personas en general, deben ser capacitados en los procedimientos de gestión de incidentes de tal manera que puedan prevenir, identificar clasificar, reportar y atender los eventos y vulnerabilidades observados.

En relación al reporte de incidentes el numeral 4.2 define:

Es obligación de cada funcionario interno o externo reportar las violaciones a las políticas de seguridad informática y a la Gestión de Incidentes de Seguridad de la Información que sean detectadas o cualquier incidente que se produzca sobre cualquier recurso informático que pueda parecer sospechoso.

Y las responsabilidades del terceros están definidas como:

Funcionarios y terceros

· Conocer y Cumplir la política, las normas y los procesos de la Gestión de Incidentes de Seguridad de la Información y reportar los incidentes

Con respecto al cumplimiento de la política, ésta indica:

En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia).

Estándares asociados a esta política

1. **Estándar de Gestión de Incidentes**

   Este estándar es una guía para funcionarios y terceros, de cómo actuar ante un incidente en Seguridad de la Información y cómo proceder en su reporte.

   "Todo el personal interno y externo de POSITIVA Compañía de Seguros debe estar en capacidad de identificar y notificar las señales de un potencial incidente. Las señales que permiten identificar la ocurrencia de un incidente se clasifican en dos categorías; indicadores y precursores:

   ***Precursor**: Es una señal de que el incidente podría ocurrir en el futuro.*
   ***Indicadores**: Es una señal que nos indica que un incidente ocurrió o está ocurriendo."*

   El inicio del incidente de seguridad de la información, se da cuando se detecta o se reportan a través de:

   · Alertas electrónicas
   · reportes mediante llamadas telefónicas,
   · correo electrónico,
   · A través de software o aplicativos para la gestión de incidentes

m. Política de Gestión de Continuidad del Negocio en TI

Esta política busca tener un guion de actividades específicas para garantizar la prestación del servicio ante eventos de falla o desastre en los sistemas de información.

El alcance indica:

- *Aplica a todos los activos de información (hardware, software, procesos, personas, información y tecnologías de información), que haga parte de los sistemas de información de POSITIVA Compañía de Seguros S.A.*
- *Está dirigida a todos los funcionarios y terceros (contratistas y proveedores) o personas que en su rol de practicantes realizan o prestan un servicio a POSITIVA Compañía de Seguros S.A.*

Con respecto al cumplimiento de la política, ésta indica:

En el caso de terceros (insourcing, outsourcing y proveedores) se aplicarán las cláusulas existentes en los contratos y dada la gravedad de los hechos se iniciarán las acciones respectivas, ante los Entes de Control pertinentes (Superintendencia Financiera de Colombia).