2014

Políticas de Seguridad de la información

JAIRO BRAVO MENDOZA
POSITIVA S.A.

Introducción

Positiva ha adoptado la norma ISO 27001 como foco de orientación para adelantar el desarrollo de las Políticas de Seguridad internas. La Norma indica 12 dominios claves en la implementación de seguridad de la información, basados en los puntos críticos de control que se deben efectuar dentro de toda organización.

A continuación se exponen cada una de ellas.

Políticas de seguridad de la información

Se identifican 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.

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 analizará cada política y sus estándares, en lo relacionado con terceros prestadores de Servicios de Información en Positiva S.A.

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 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 dice:
*"**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:
•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.

c. Política de Seguridad Física y Ambiental

Esta política implica el mantener control de acceso a los locales 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 indica:
"· 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"

d. Política de Cumplimiento de requisitos legales en TI

Esta política propende a la observancia de la regulación nacional vigente con respecto a 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 empleado, terceros y clientes y velar por que los terceros protejan la información de carácter personal de clientes o funcionarios, que le sea entregada por el objeto del contrato para su procesamiento.

e. 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. esta 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."

f. 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.

g. 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 norma 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 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).

h. 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).

i. 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).

j. 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 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 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).

l. 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).