Versión: 2.0
Fecha Última Actualización: 28/11/2017
Aprobado por: Vicepresidencia Riesgos
Fecha de Publicación: 28/11/2017
Área Responsable: Gerencia Riesgos Colombia

Lineamientos de seguridad de la información para proveedores

1. Marco de referencia

Este documento define los lineamientos de seguridad de la información para la gestión de proveedores con acceso a la información. Hace parte integral de la política general de seguridad como una especificación de sus lineamientos.

Contempla prácticas exitosas incorporadas a partir de normas internacionales de seguridad que la organización ha seleccionado para su cumplimiento o referencia, así como lineamientos externos definidos por los diferentes entes de control que regulan nuestras actividades.

En este documento cuando se haga referencia a *Las Compañías* se habla de Suramericana S.A y sus filiales en Colombia.

2. Alcance

Los lineamientos definidos en este documento aplican para todos los proveedores cuyo objeto de trabajo les dé acceso a la información de *Las Compañías*.

3. Glosario

Clasificación de la información de *Las Compañías,* según el estándar definido es*:*

Información De Dominio Público: Es la información que ha sido declarada de conocimiento público por parte del Dueño del Activo de Información. Este tipo de información puede ser entregada o publicada a todo tipo de público (personas internas, externas de *Las Compañías* y miembros de la competencia) sin restricciones y sin que esto implique daños a los grupos de interés, a las actividades, a los procesos de *Las Compañías.*

Información De Uso Interno: Es la información que utilizan los empleados de *Las Compañías* para realizar las operaciones diarias del negocio y que no puede ser

conocida por terceros sin previa autorización del Dueño del Activo de Información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de manera leve a terceros, a los sistemas y/o procesos de *Las Compañías.*

Información Restringida: Es información de *Las Compañías* que es utilizada sólo por un grupo de empleados, colaboradores o terceros para realizar sus labores y que no puede ser conocida por otros empleados, colaboradores o terceros sin autorización del Dueño del Activo de Información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante cualquiera de los grupos de interés de *Las Compañías* (accionistas, empleados, clientes, proveedores) o a los sistemas y/o procesos de *Las Compañías.*

Información Confidencial: Es aquella información que se encuentra definida por la ley, las regulaciones o el Dueño del Activo de Información como representante de *Las Compañías.* Esta información únicamente puede ser conocida, utilizada y modificada por cualquier empleado y/o colaborador de *Las Compañías* que lo requiera en función de su trabajo, con previa autorización del Dueño del Activo de Información. Se debe llevar un registro de las consultas y/o modificaciones realizadas por los Usuarios de la información confidencial.
Para el caso específico de *Las Compañías*, se considera confidencial la información contenida en las Historias Clínicas, información que contenga datos sensibles, entendiendo como dato sensible, información que afecte la intimidad o pueda generar discriminación como: origen racial o étnico, orientación política o que promuevan intereses políticos, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como también cualquier información que contenga la cédula o NIT del cliente.

4. Declaración

Todos los proveedores, deben dar cumplimiento a la política, directrices y lineamientos de seguridad, establecido por *Las Compañías* en el marco normativo de seguridad, para la protección de su información y no incurrir en conductas que

generen riesgos o puedan ocasionar incidentes que afecten a la información o la operación.

5. Lineamientos.

5.1. Contratación de los proveedores

5.1.1. Siempre que un proceso de negociación, licitación o selección implique la entrega al proveedor de información de uso interno, restringida o confidencial, se deberá firmar previamente el acuerdo de confidencialidad establecido por *Las Compañías*.

5.1.2. Una vez el proveedor sea contratado y requiera acceso a la información de uso interno, restringida o confidencial de *Las Compañías*, debe celebrar el acuerdo de confidencialidad establecido por *Las Compañías o incorporar dentro del contrato la cláusula correspondiente*. Así mismo, en el contrato deben definirse los procedimientos y responsabilidades que deben surtirse con la información que poseen de Las Compañías durante la vigencia y terminación del contrato.

5.2. Información del proveedor

5.2.1. *Las Compañías* se comprometen a salvaguardar la información de negocio de los proveedores, no revelando información sobre los mismos a otras partes sin su autorización explícita.

5.3. Administración de proveedores con acceso a información[1]

5.3.1. Todos los proveedores están obligados a cumplir con las políticas, directrices, lineamientos y en general todas las actividades que *Las Compañías* establezcan dentro del marco normativo de seguridad como necesarias para proteger su información y operación.

5.3.2. Todo proveedor con acceso a la información de las Compañías debe cumplir con el proceso de inscripción de proveedores, así como con las demás disposiciones establecidas por *Las Compañías* para su relacionamiento y administración.

5.3.3. Los proveedores que tengan acceso a la información deben participar en las iniciativas de concientización y capacitación en materia de seguridad de la información a las que sea convocados.

5.4. Comportamiento seguro

5.4.1. El uso de la información y/o los recursos informáticos está restringido única y exclusivamente para propósitos laborales.

[1] Se refiere a información de uso interno, uso restringido o confidencial.

5.4.2. Todas las personas son responsables de garantizar la debida protección de la información y de los recursos asignados según su clasificación y los estándares definidos para ello.

5.4.3. Las personas no pueden por ningún motivo vender, transferir o intercambiar información de *Las Compañías* sin cumplir con los procedimientos de aprobación definidos.

5.4.4. Todos los **recursos de información** son monitoreados y pueden ser auditados cuando el personal o área designada por *Las Compañías* lo considere.

5.4.5. Está prohibido crear, acceder, almacenar, distribuir, vender, instalar o transmitir **material ilegal** o pornográfico por medio de los recursos informáticos de *Las Compañías*.

5.4.6. Está prohibido el uso de los recursos de *Las Compañías* para realizar acciones malintencionadas, tales como, amenazas o ataques de seguridad de la información, al interior de las mismas o a terceros.

5.4.7. Está prohibido eludir los controles de seguridad que *Las Compañías* establezcan para la protección de la información o someterlos a prueba sin las debidas autorizaciones.

5.4.8. Todas las condiciones que puedan afectar a la seguridad de la información (vulnerabilidades, amenazas, riesgos, eventos, incidentes) que se identifiquen, deben ser reportadas a correo de Incidentes de Seguridad IncidentesSeguridad@suramericana.com.co .

5.4.9. Toda persona al terminar su relación contractual con alguna de *Las Compañías* debe devolver la información y activos que sea propiedad de las mismas.

5.4.10. Toda contratación de desarrollo, mantenimiento, compra, entre otros, de sistemas de información, aplicaciones o infraestructura tecnológica debe contar con el acompañamiento de las áreas de TI y debe seguir el marco normativo de seguridad, definido para ello.

5.5. Equipos de cómputo asignados

5.5.1. Únicamente las personas autorizadas por *Las Compañías* pueden modificar las configuraciones de los **equipos de cómputo**, descargar o instalar software.

5.5.2. Únicamente se pueden establecer conexiones **desde equipos de proveedores a equipos o servicios productivos** de *Las*

Compañías, si se siguen los procedimientos de seguridad requeridos y se cuenta con la respectiva autorización.

5.5.3. Los **equipos de cómputo** asignados por *Las Compañías* no pueden ser objeto de cambios en sus componentes físicos.

5.5.4. Las personas no están autorizadas a entregar o prestar el equipo de cómputo a terceros no relacionados con *Las Compañías*.

5.5.5. Todos los usuarios deben bloquear el equipo de cómputo asignado cuando no se encuentren bajo su supervisión.

5.5.6. Los usuarios deben reportar cualquier daño o pérdida del equipo de cómputo asignado a su jefe inmediato y al área de Soporte de Servicios tecnológicos. En caso de hurto o pérdida se debe realizar el respectivo denuncio ante las autoridades pertinentes.

5.5.7. Todos los usuarios con equipo portátil asignado por *Las Compañías* deben asegurarlo adecuadamente al puesto de trabajo con el cable antirrobo de seguridad o guardarlo bajo llave cuando se encuentre ausente del puesto de trabajo.

5.5.8. Los equipos asignados no cuentan con copias de respaldo de la información, la información corporativa debe ser almacenada en los medios asignados para este fin. (carpetas compartidas, SharePoint, archivo físico, entre otros).

5.6. Antivirus

5.6.1. Cualquier persona que sospeche que su equipo asignado ha sido infectado por un virus debe inmediatamente comunicarse con la línea de atención 7090, para reportar la situación y recibir el soporte adecuado.

5.6.2. Los servicios de antivirus en los equipos de cómputo asignados por *Las Compañías* no se pueden alterar, detener o desinstalar.

5.7. Correo electrónico

5.7.1. Las cuentas de correo electrónico suministradas por *Las Compañías* deben ser utilizadas únicamente para propósitos laborales de la organización.

5.7.2. Los usuarios son responsables del contenido que se envíe a través del correo corporativo.

5.7.3. Sólo el personal autorizado por *Las Compañías* puede enviar **correos masivos** a través del correo electrónico corporativo.

5.7.4. Los correos sospechosos se deben reportar al buzón de correo no deseado correond@suramericana.com.co para el tratamiento de dicho riesgo.

5.7.5. Las personas no deben usar su cuenta de correo electrónico corporativo para afiliarse a servicios o productos personales o que no esté relacionado con las funciones de su cargo.

5.8. Internet

5.8.1. El internet es de uso exclusivo para las labores de *Las Compañías.*

5.8.2. La información confidencial, restringida o de uso interno de *Las Compañías,* no podrá estar en sitios públicos en Internet. (Por ejemplo: Dropbox, Drive, Wetransfer, Prezi, Pastebin, Slideshare, Googledocs, entre otras), sin la debida autorización del dueño de la información y siguiendo las medidas de seguridad definidas.

5.9. Servicios de almacenamiento

5.9.1. La información crítica del negocio debe ser almacenada en los **servicios de almacenamiento de información provistos por las compañías**.

5.9.2. Está prohibido el almacenamiento de información personal en **servicios de almacenamiento de información provistos por las compañías**.

5.9.3. Sólo se realiza copia de respaldo a la información contenida en los **servicios de almacenamiento de información provistos por las compañías**.

5.10. Áreas de trabajo

5.10.1. Las personas [2] deben mantener en un lugar visible las identificaciones que los acrediten como proveedores y cumplir con los lineamientos definidos por seguridad física para el acceso a las distintas sedes.

5.10.2. Las personas [3] deben acceder sólo a las áreas a las que se encuentren autorizadas.

5.10.3. Las personas deben proteger la información restringida, confidencial o de uso interno en las áreas de trabajo.

5.11. Uso de redes sociales externas.

[2]Hace referencia a proveedores con acceso a información
[3]Hace referencia a proveedores con acceso a información

5.11.1. Los proveedores con acceso a información no deben publicar información de *Las Compañías* en redes sociales externas sin la debida autorización.

5.11.2. Los colaboradores no deben realizar publicaciones que atenten contra el buen nombre de la organización o sus empleados.

5.11.3. El uso de redes sociales para temas relacionados con la imagen corporativa se debe realizar bajo los parámetros definidos por las áreas de mercadeo.

5.12. Información de reuniones

5.12.1. Cuando se requiera grabar en audio o video las reuniones de trabajo o teleconferencias, se debe notificar y solicitar el consentimiento de los participantes. El almacenamiento de esta información debe cumplir el marco Normativo de Seguridad y quedar bajo responsabilidad de quien la realiza.

5.12.2. En los espacios para reuniones dispuestos por *Las Compañías* no se debe dejar información. Por ejemplo, En los tableros de las salas de reuniones, en los televisores o proyectores, documentos, entre otros

5.13. Privilegios de acceso y cuentas de usuario

5.13.1. Las credenciales de acceso (usuario y contraseña, tarjeta de acceso físico, entre otros) son de uso personal e intransferible.

5.13.2. Es responsabilidad de cada persona las acciones ejecutadas con su usuario y contraseña en las aplicaciones y plataformas de *Las Compañías.*

5.13.3. Las personas que poseen más privilegios de acceso de los que corresponden a las funciones desempeñadas en *Las Compañías*, deben reportarlo a su Jefe inmediato o responsable del contrato en *Las Compañías.*

5.13.4. Los usuarios no deben escribir las contraseñas en medios físicos o electrónicos de fácil acceso para otras personas.

5.13.5. Los usuarios tienen la responsabilidad de cambiar su contraseña periódicamente, como máximo cada 90 días.

5.13.6. En caso que el usuario detecte o sospeche que su contraseña fue conocida por un tercero, debe cambiarla de manera inmediata y reportar el incidente al correo de Incidentes de Seguridad IncidentesSeguridad@suramericana.com.co

5.13.7. Los usuarios deben usar contraseñas seguras para sus accesos, teniendo en cuenta los siguientes requisitos:

-Mínimo ocho caracteres.
-No contener únicamente el nombre de usuario, el nombre real o el nombre de la empresa.
-Debe ser significativamente diferente de las últimas cinco contraseñas utilizadas.
-Estar compuesta por caracteres de cada una de las siguientes categorías: letras mayúsculas, letras minúsculas y números[4].

6. Gobernabilidad:

Este documento se rige bajo los lineamientos de la política general de seguridad de la información aprobada por el órgano competente en *Las Compañías.*

7. Instancias de decisión:

Las instancias de decisión del marco normativo de seguridad serán las definidas en la política general de seguridad de información.

8. Divulgación:

La presente definición será vinculante y deberá ser publicada a todos los grupos de interés, dentro de los sitios definidos por *Las compañías*.
Las compañías manejan información que está legalmente protegida por normas específicas, por tanto un uso indebido de la misma, podrá acarrear sanciones legales sobre *Las Compañías* o sus grupos de interés.

[4] Cuando la plataforma lo permita incluir caracteres especiales, como los siguientes: *,+,[,#,%,&,/

Versión: 2.0
Fecha Última Actualización: 28/11/2017
Aprobado por: Vicepresidencia Riesgos
Fecha de Publicación: 28/11/2017
Área Responsable: Gerencia Riesgos Colombia

CONTROL DE CAMBIOS			
FECHA	**VERSIÓN**	**AUTOR**	**DESCRIPCIÓN DEL CAMBIO**
17/07/2017	1.0	Leidy Tatiana Vélez Analista de seguridad de la Información	Creación del documento
24/08/2017	1.0	Leidy Tatiana Vélez Analista de seguridad de la Información Área de Asuntos legales – Contrataciones Seguridad Social	Actualización
28/11/2017	2.0	Leidy Tatiana Vélez Analista de seguridad de la Información Área de Asuntos legales: Contrataciones Seguridad Social, Contrataciones Seguros Área de proveedores de negocio	Consolidación de lineamientos
28/11/2017	2.0	Marcela Jimenez Directora de Riesgos Operacionales	Aprobación del documento
28/11/2017	2.0	Leidy Tatiana Vélez Analista de seguridad de la Información	Divulgación y publicación en la intranet