Coltefinanciera S.A. COMPAÑIA DE FINANCIAMIENTO	INSTRUCTIVO PARA LA FORMACIÓN DE PROVEEDORES EN EL SGSI

Revisó:	Aprobó:
WILDER ALEXANDER MEJIA Oficial de Seguridad de la información	WILLIAM BURBANO BERNAL Gerente de Riesgo Operativo
Fecha: 19-11-2013	Fecha: 23-01-2014

INSTRUCTIVO PARA LA FORMACIÓN DE PROVEEDORES

CONTROL DE CAMBIOS		
FECHA	**DESCRIPCIÓN DEL CAMBIO**	**VERSIÓN ACTUAL**
19-11-2013	Creación del Documento	01

INTRODUCCIÓN

Este instructivo pretende servir de medio, para la sensibilización de los terceros contratados por COLTEFINANCIERA S.A., reglamentando la forma en que la Compañía previene, protege y maneja los riesgos de seguridad de la información en diversas circunstancias. Las normas y políticas expuestas en este instructivo son de estricto cumplimiento y deben darse a conocer a todos los empleados del contratista que tengan algún vínculo con la Compañía.

OBJETIVOS

- Dar a conocer las políticas para el uso seguro de la información y de los activos de información.
- Especificar las políticas para el intercambio seguro de la información.
- Instruir a los terceros en los lineamientos para la clasificación y etiquetado de la información.

ALCANCE

Aplica para los terceros contratados por COLTEFINANCIERA S.A. que en desarrollo de su actividad tengan acceso a información de la Compañía y/o servicios de procesamiento de información.

1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ACTIVIDADES:			
N°	**DESCRIPCION**	**FUENTE DE INFORMACIÓN**	**RESPONSABLE**
1.1	Los terceros que requieran recursos para el ejercicio de sus funciones deben solicitarlo de acuerdo con el PR-M12-P1-01 Procesos básicos de la administración del Talento Humano o el PR-M9-P2-01 Compras y evaluación de proveedores en el momento de la contratación	Políticas de Seguridad de la Información	Terceros
1.2	Los terceros que requieran acceso y privilegios a la red y servicios de sistemas de información, deben solicitarlo de acuerdo con el PR-M13-P3-02 Procedimiento de control de acceso.	Políticas de Seguridad de la Información	Terceros
1.3	Recomendaciones para el buen manejo de la contraseña: • Debe tener mínimo 10 caracteres. • Se debe cambiar máximo cada 45 días • El sistema conserva un historial 5 contraseñas, por lo tanto no se permite repetir ninguna de las contraseñas almacenadas en esté. • La contraseña debe ser compleja, es decir que tenga combinaciones de caracteres numéricos y alfanuméricos mayúsculas y minúsculas • La contraseña al tercer intento inválido se bloquea.	Políticas de Seguridad de la Información	Terceros
1.4	La contraseña es responsabilidad absoluta del usuario. Por tanto su uso es personal e intransferible	Políticas de Seguridad de la Información	Terceros
1.5	La información confidencial intercambiada con COLTEFINANCIERA S.A. debe ser cifrada. En todo momento se debe garantizar que se utilizan mecanismos de cifrado fuerte.	Políticas de Seguridad de la Información	Terceros

ACTIVIDADES:			
N°	**DESCRIPCION**	**FUENTE DE INFORMACIÓN**	**RESPONSABLE**
1.6	Los terceros que tengan acceso al correo corporativo deberán seguir las siguientes directrices: • Por ningún motivo se puede enviar a través del correo electrónico corporativo material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar o de cualquier otra manera, censurable • El límite establecido para el envío y recepción de correos corporativos es de 20 Mb. • Los correos transmitidos son correspondencia privada entre el destinatario y el remitente. Por lo tanto cualquier conducta de interceptación, modificación, alteración o apropiación de mensajes, será considerado una falta grave. • No está permitido registrar la cuenta de correo corporativo, en páginas Web o cualquier otro medio de uso personal	Políticas de Seguridad de la Información	Terceros
1.7	Los terceros que tengan acceso a internet deberán seguir las siguientes directrices: • No es permitido el uso de servicios de Internet para explorar páginas con contenidos ilegales, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar o de cualquier otra manera, censurable. • No se permite la descarga, ejecución e instalación de ningún tipo de programas o aplicaciones encontradas en Internet. Todo cambio en la configuración de la estación de trabajo debe realizarse a través de la Gerencia de Procesos y Tecnología • No se permite la descarga de contenidos fuera del alcance del objeto del trabajo como música, videos, juegos o películas. • No está permitido el acceso a redes sociales, correos personales y mensajería instantánea externa (Chat).	Políticas de Seguridad de la Información	Terceros
1.8	COLTEFINANCIERA S.A. podrá monitorear y supervisar los sistemas, servicios y equipos, de acuerdo con lo establecido en las políticas de seguridad de la Compañía y en cualquier proceso legal que se requiera.	Políticas de Seguridad de la Información	Terceros
1.9	Los terceros que se les asigne una estación de trabajo proporcionadas por la Compañía deberán seguir las siguientes directrices: • Se prohíbe modificar o intentar hacer cambios en la configuración de seguridad de la estación de trabajo.	Políticas de Seguridad de la Información	Terceros

ACTIVIDADES:			
N°	**DESCRIPCION**	**FUENTE DE INFORMACIÓN**	**RESPONSABLE**
	• Todos los contratistas y consultores después de la terminación o expiración de su contrato, deben someterse a lo estipulado en el convenio de confidencialidad firmado. • Los terceros no deben escribir, generar, compilar, copiar, recopilar, difundir, ejecutar, o intentar introducir cualquier código de computadora diseñado para auto-replicarse, dañar o afectar el correcto desempeño de cualquier computador o red de Coltefinanciera S.A.		
1.10	La conexión para trabajo remoto debe realizarse según el PR-M13-P3-02 ANEXO 02 Directrices de acceso remoto del procedimiento de PR-M13-P3-02 control de acceso para el servicio de VPN o el que se tenga dispuesto por la Gerencia de Procesos y Tecnología.	Políticas de Seguridad de la Información	Terceros
1.11	Se prohíbe la instalación de dispositivos de almacenamiento masivo, a menos que las funciones a realizar lo permita según lo establecido por el Comité de Seguridad de Información.	Políticas de Seguridad de la Información	Terceros
1.12	Los terceros que requieran acceso a la información de la Compañía deberán firmar un convenio de confidencialidad.	Políticas de Seguridad de la Información	Terceros
1.13	Se deberá solicitar autorización de forma escrita, para acceder a la información confidencial por parte del Propietario del Activo, Comité de seguridad de la información o Junta Directiva.	Políticas de Seguridad de la Información	Terceros
1.14	Los terceros, deben portar su identificación de manera visible durante el tiempo que permanezca dentro de las instalaciones de la compañía, así mismo no se permite la conexión a la red corporativa de equipos de su propiedad como (Portátil, Tablets, SmartPhone, Etc.)	Políticas de Seguridad de la Información	Terceros

ACTIVIDADES:			
N°	**DESCRIPCION**	**FUENTE DE INFORMACIÓN**	**RESPONSABLE**
1.15	Todos los terceros que utilicen sistemas, servicios, y equipos (ej. Estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de COLTEFINANCIERA S.A., deben reportar cualquier situación que se pueda considerar como un evento de seguridad y que comprometa la preservación de la confidencialidad, disponibilidad y/o integridad de la información, por los siguientes medios: a. SARO: Sistema de administración de Riesgo Operativo. b. SAC: Servicio de atención al cliente interno. c. Correo electrónico: SGSI@coltefinanciera.com.co, canaletico@coltefinanciera.com.co, seguridadit@coltefinanciera.com.co d. Línea telefónica Extensiones: 6111, 6150, 6005 e. Línea Ética 01800 01800 56 Se considera un evento de seguridad la ocurrencia de una situación que indica una posible violación a las políticas de seguridad de la información o fallas en los controles que no genere un impacto en el desarrollo de las operaciones de la organización y que puede ser controlado rápidamente. Se considera un incidente de Seguridad de la información, la ocurrencia de un acto intencional o no intencional que tiene una alta probabilidad de afectar el buen funcionamiento de los sistemas de información, que a causa de este acto se vea afectada la operación de la entidad y que por lo tanto amenaza la seguridad de la información.	Políticas de Seguridad de la Información	Terceros

2. POLÍTICAS DE GESTIÓN DE LA INFORMACIÓN.

<table>
<tr><th colspan="4">ACTIVIDADES:</th></tr>
<tr><th>N°</th><th>DESCRIPCIÓN</th><th>FUENTE DE INFORMACIÓN</th><th>RESPONSABLE</th></tr>
<tr><td>2.1</td><td>La información de Coltefinanciera S.A. se clasifica de acuerdo a la siguiente tabla:

<table><tr><th>CLASIFICACIÓN DE LA INFORMACIÓN</th><th>DEFINICIÓN</th></tr><tr><td>Información pública</td><td>Esta información ha sido expresamente aprobada por la Alta Dirección como adecuada para la difusión pública, tal como quedo clasificada en el inventario de activos de información.</td></tr><tr><td>Información para uso interno</td><td>Esta información es de libre acceso a todos los empleados, solo debe ser divulgada a terceros si se ha firmado un acuerdo de confidencialidad. Esta es la clasificación por defecto para cualquier información no explícitamente designada.</td></tr><tr><td>Información confidencial</td><td>El acceso a esta información debe ser estrictamente restringido basado en el concepto de la indispensable necesidad de saber. La divulgación de la información requiere la aprobación del propietario y en el caso de ser revelada a terceros, debe firmarse también un acuerdo de confidencialidad.</td></tr></table></td><td>Políticas de Gestión de la Información</td><td>Terceros</td></tr>
<tr><td>2.2</td><td>De acuerdo a la clasificación de la información esta se debe etiquetar de la siguiente manera:

<table><tr><th>CLASIFICACIÓN</th><th>INFORMACIÓN IMPRESA</th><th>INFORMACIÓN ELECTRÓNICA</th></tr><tr><td>Información pública</td><td>No requiere etiquetado</td><td>No requiere etiquetado</td></tr><tr><td>Información para uso interno</td><td>Etiqueta o marca de “Solo de uso interno”</td><td>Nombre del archivo o carpeta con la palabra “Solo de uso interno”</td></tr><tr><td>Información confidencial</td><td>Etiqueta o marca de “Confidencial”</td><td>Nombre del archivo o carpeta con la palabra “confidencial”
Rótulo de confidencial en el medio de almacenamiento (CD o DVD)
Correo electrónico rotulado en el asunto como “confidencial”</td></tr></table></td><td>Políticas de Gestión de la Información</td><td>Terceros</td></tr>
</table>

ACTIVIDADES:

<table>
<tr><th>N°</th><th>DESCRIPCIÓN</th><th>FUENTE DE INFORMACIÓN</th><th>RESPONSABLE</th></tr>
<tr><td>2.3</td><td>Para garantizar la seguridad en el intercambio de información se tienen establecidas las reglas de distribución, receptores autorizados y medios de transferencia.
Los controles de intercambio de información según la clasificación se describen en la siguiente tabla:
<table>
<tr><th>ACCESO</th><th>EN MEDIO FÍSICO</th><th>INTERCAMBIO ELECTRÓNICO</th><th>MEDIOS DE ALMACENAMIENTO</th><th>TELEFÓNICO / FAX</th></tr>
<tr><td>Información pública</td><td>Sin restricción de intercambio.</td><td>Sin restricción de intercambio.</td><td>Sin restricción de intercambio.</td><td>Sin restricción de intercambio.</td></tr>
<tr><td>Información para uso interno</td><td>Sobre sellado en mensajería normal con control de envío y recepción.</td><td>Servicio de correo de la organización (no por correo personal).
Con nota pie de página en el correo (Disclaimer de confidencialidad)</td><td>Sobre sellado en mensajería normal con control de envío y recepción</td><td>Solo se permite la comunicación telefónica entre sedes y agencias.</td></tr>
<tr><td>Información confidencial</td><td>Registro de control de envío.
Sobre sellado con etiquetado de “Confidencial”</td><td>Servicio de correo de la organización con la Información cifrada.
Con nota pie de página en el correo (Disclaimer de confidencialidad)</td><td>Registro de Control de envío de medios con la información cifrada.
Sobre sellado con etiquetado de “Confidencial”</td><td>Solo se permite la comunicación telefónica entre sedes y agencias.</td></tr>
</table></td><td>Políticas de Gestión de la Información</td><td>Terceros</td></tr>
<tr><td>2.4</td><td>La información debe enviarse considerando los controles que se definen a continuación:
<table>
<tr><th>MEDIO</th><th>EMPAQUETADO</th><th>IDENTIFICACIÓN Y ETIQUETADO</th><th>MEDIO DE TRANSPORTE</th><th>OTRAS REGLAS DE USO</th></tr>
<tr><td>Correo en medio físico</td><td>Sobre sellado o caja de cartón que oculte contenido. El empaque debe ser tal que evite daño o deterioro.</td><td>Identificación de la organización y remitente en el sobre.
Etiquetado de “confidencial”, cuando se trate de información confidencial.</td><td>Empresa de mensajería aprobada por área administrativa y con acuerdo de confidencialidad.</td><td>Información confidencial debe entregarse personalmente, por medio de un correo certificado.</td></tr>
</table></td><td>Políticas de Gestión de la Información</td><td>Terceros</td></tr>
</table>

ACTIVIDADES:

N°	DESCRIPCIÓN	FUENTE DE INFORMACIÓN	RESPONSABLE

MEDIO	EMPAQUETADO	IDENTIFICACIÓN Y ETIQUETADO	MEDIO DE TRANSPORTE	OTRAS REGLAS DE USO
Transporte de medios de almacenamiento (USB, Medios ópticos, cintas, dispositivos de almacenamiento extraíbles.)	Sobre sellado o caja de cartón que oculte contenido. El empaque debe ser tal que evite daño o deterioro del medio.	Identificación de la organización y remitente en el sobre. La información confidencial debe estar cifrada.	Empresa de mensajería aprobada por área administrativa y con acuerdo de confidencialidad	Información confidencial debe entregarse personalmente, por medio de un correo certificado.
Intercambio electrónico	N/A	El mensaje debe contener: Remitente, Cargo, Organización y Disclaimer de Confidencialidad. Cuando se trate de información confidencial la etiqueta de “Confidencial” y esta debe ser cifrada.	Servicio interno de mensajería electrónica y correo. Solo se permite el acceso a correos externos de aquellos proveedores que tengan un contrato firmado y un convenio de confidencialidad.	Se aplican los procedimientos y políticas de seguridad en la red
Telefonía fija y celular.	N/A	N/A	Proveedor de servicios de telefonía aprobado y con el respectivo convenio de confidencialidad firmado.	Garantizar las medidas necesarias al transmitir información confidencial por este medio.
Fax	N/A	Encabezado de fax debe incluir: Remitente, Cargo y Organización. Etiquetado de “confidencial”, cuando se trate de información confidencial.	Proveedor de servicios de telefonía aprobado y con el respectivo convenio de confidencialidad firmado.	Garantizar las medidas necesarias al transmitir información confidencial por este medio.

<table>
<tr><th colspan="4">ACTIVIDADES:</th></tr>
<tr><th>N°</th><th>DESCRIPCIÓN</th><th>FUENTE DE INFORMACIÓN</th><th>RESPONSABLE</th></tr>
<tr><td>2.5</td><td>La autorización de copia de la información se determina en función del nivel de acceso, teniendo en cuenta las disposiciones para cada proceso. La autorización de copias según el nivel de acceso se describe a continuación:

<table><tr><th>ACCESO</th><th>COPIAS AUTORIZADAS</th></tr><tr><td>Información pública</td><td>No se requiere autorización de copias.</td></tr><tr><td>Información para uso interno</td><td>Pueden hacerse copias bajo responsabilidad del propietario, considerando los riesgos posibles y el procedimiento de control de documentos y registros.</td></tr><tr><td>Información confidencial</td><td>Se requiere autorización del propietario del activo.</td></tr></table></td><td>Políticas de Gestión de la Información</td><td>Terceros</td></tr>
<tr><td>2.6</td><td>Toda la correspondencia de la organización debe ser tramitada a través de Administración de Documentos. La información que sea de carácter confidencial, deberá tener el respectivo rótulo o sello que indique el tipo de información. Los empleados de ésta área deben tener los respectivos acuerdos de confidencialidad ya que la información que ingresa a la Compañía, debe ser analizada por ellos antes de darle el trámite respectivo.</td><td>Políticas de Gestión de la Información</td><td>Terceros</td></tr>
</table>

3. INCUMPLIMIENTO DE LAS POLÍTICAS.

El incumplimiento de estas políticas puede traer consecuencias de tipo jurídico y legal y en su defecto la cancelación del contrato.