COBERTURAS

Desde 1978

Personas sirviendo a Personas!

globex INTERNATIONAL GROUP
International Risk Management
International Benefits Consulting

POLITICA
DE SEGURIDAD DE LA INFORMACION

VIGILADO Superintendencia Financiera

BLA DE CONTENIDO

1. INTRODUCCION

Las políticas de seguridad definidas en el presente documento están dirigidas a los empleados de Sociedad de Coberturas Ltda, las cuales serán de obligatorio cumplimiento, a fin de proteger la información y otros activos informáticos de amenazas y vulnerabilidades y garantizar la integridad, confidencialidad y disponibilidad de la información.

Con la definición de las políticas y estándares de seguridad informática, se busca establecer en el interior de Sociedad de Coberturas una cultura de excelencia en la calidad operando en una forma confiable.

2. DEFINICION DE SEGURIDAD DE LA INFORMACION

La información es considerada un activo esencial en las actividades de la organización, es por ello que se deben establecer estrategias que permitan el control y administración de los datos, así como el uso adecuado de los recursos informáticos tanto de Hardware como de Software. De ahí la importancia de definir y dar a conocer políticas y procedimientos de seguridad que permitan proteger los Sistemas de Información de las amenazas a las que se encuentra expuesto por el uso de tecnologías de la información y asegurar la continuidad de los procesos y el logro de los objetivos institucionales.

3. OBJETIVO

Las políticas de seguridad informática comprenden un conjunto de reglas a ser aplicadas a todas las actividades relacionadas con los sistemas de información que soportan los procesos críticos de Sociedad de Coberturas, con el objeto de:

- ✓ Garantizar la integridad, confidencialidad y disponibilidad de la información
- ✓ Proteger los recursos tecnológicos.
- ✓ Minimizar el riesgo en los procesos críticos de la Entidad
- ✓ Cumplir con los principios de la función Administrativa
- ✓ Apoyar la innovación tecnológica
- ✓ Implementar el Sistema de Gestión de la Seguridad Informática SGSI
- ✓ Fortalecer la cultura de autocontrol de la información
- ✓ Garantizar la continuidad de los procesos frente a los incidentes.

4. ALCANCE

Las políticas de seguridad informática y controles serán de obligatorio cumplimiento para todos los empleados, contratistas y terceros que hagan uso de los activos de información de Sociedad de Coberturas.

El incumplimiento al presente documento, podrá presumirse como causa de responsabilidad administrativa y/o disciplinaria, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por la Gerencia de la Compañía sin exceptuar cualquier violación a normas legales vigentes en el código penal u otros textos.

Las excepciones al cumplimiento de las políticas de seguridad informática serán autorizadas única y exclusivamente por la Gerencia de la Compañía, cuando se considere que su impacto es negativo para la continuidad de los procesos o logro de los objetivos de la empresa, y deberán ser documentadas formalmente.

Las políticas de seguridad informática serán objeto de evaluación semestral, aplicando mecanismos de autocontrol y autoevaluación, para garantizar el mejoramiento continuo.

5. REQUISITOS LEGALES Y/O REGLAMENTARIOS

LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República.

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY 1266 DE 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1273 DE 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.

DECRETO 2609 DE 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

DECRETO 2693 DE 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones.

DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:20013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

LEY 1712 DE 2014; Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones.

DECRETO 103 DE 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

DECRETO 1494 DE 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014.

6. TERMINOLOGIA Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la empresa.
Administrador de equipo: Persona responsable de configurar, administrar controladores de dominio o equipos locales, sus cuentas de usuario, asignar contraseñas, permisos y ayudar a los usuarios a solucionar problemas de red.
Administrador de Bases de Datos (DBA): Persona responsable de los aspectos ambientales de una base de datos.
Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
Backups: Es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.
Base de Datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.
Control de Acceso: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.
Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.
Hardware: Se refiere a las características técnicas y físicas de las computadoras.
Integridad: Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.
IP: Etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP.
Plan de Contingencia: Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.
Redes: Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.
Servidores: Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la

arquitectura cliente-servidor.
SGSI: Sistema de Gestión de Seguridad de la Información
Sistemas de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.
Software: Programas y documentación de respaldo que permite y facilita el uso del PC. El software controla la operación del hardware.
Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

7. POLITICAS Y CONTROLES

7.1. POLITICA GENERALES DE SEGURIDAD DE LA INFORMACION

Sociedad de Coberturas Ltda ha establecido las siguientes políticas de seguridad, las cuales representan el interés de la Administración de proteger los Activos de Información.

7.1.1 Las políticas de seguridad de la información estarán contenidas en un documento que surtirá el trámite de aprobación de conformidad con el procedimiento de control de documentos y será publicado y comunicado a todos los empleados por parte de la Gerencia General.

7.1.2 Las políticas de seguridad información serán objeto de evaluación anual, aplicando mecanismos de autocontrol y autoevaluación, para garantizar el mejoramiento continuo.

Objetivo: Proveer la información necesaria a los usuarios sobre las políticas y controles a aplicar para hacer uso de los recursos de Internet y portal Web de Sociedad de Coberturas.
Política: En Sociedad de Coberturas el acceso a Internet es permitido a todos los empleados para facilitar el desarrollo de los procesos propios de la Entidad, no obstante están obligados a cumplir con los controles de acceso y uso implementados por la Gerencia.
Finalidad del uso de internet: los canales de acceso a internet de la Empresa no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Empresa o de las personas.

Sociedad de Coberturas se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

El uso de Internet para la revisión de correo electrónico personal, en cumplimiento de actividades propias de la Empresa, está autorizado siempre y cuando se observen los mismos lineamientos estipulados para la utilización del servicio de correo interno.

Publicación Portal Web
Administración de los Contenidos Institucionales de las Páginas: La administración de los contenidos de las páginas institucionales estará a cargo del Gerente de la empresa, quien será el encargado de verificar los contenidos que pueden o deben ser publicados. Todo contenido deberá respetar la ley de derechos de autor.

Ningún contenido del portal WEB se puede copiar con fines comerciales, ni se puede copiar y utilizar en otros sitios WEB.

Restricción para descarga de Software: La actividad de descarga de software estará a cargo de la Subgerencia, por lo tanto los usuarios de internet no están autorizados para descargar software, música, juegos, películas, protectores de pantalla, etc. Así como efectuar pagos, compras de bienes o servicios a través de los canales de acceso a internet de Sociedad de Coberturas a título personal o de la Entidad,.

Los Usuarios de Internet no están autorizados para descargar herramientas que comprometan la seguridad con actos como monitoreo de datos, sondeo, copias, prueba de firewalls o hacking entre otros.

CONFIGURACION Y ADMINISTRACION DE LAS REDES

Política: La Gerencia delegará a personal capacitado, responsable de la configuración y administración de las redes de tal forma que se garantice el control de acceso y la restricción de privilegios, dando aplicación al protocolo que se establezca para tal fin.

Política: Los empleados de Sociedad de Coberturas no deben establecer redes de área local, conexión remota a redes internas o externas, utilizando la red de la Entidad sin autorización previa de la Gerencia.

Controles

El acceso a la Red Inalámbrica de Sociedad de Coberturas a través de equipos de telefonía móvil será restringido por la Gerencia, a fin de minimizar los riesgos y mejorar la velocidad en la navegación desde equipos portátiles, siendo este el fin principal de este tipo de tecnología.

CONTROL DE ACCESOS

ADMINISTRACION DE CONTRASEÑAS Y CONTROL DE ACCESO LOGICO

Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas de información.

Política: Las tareas realizadas por los usuarios en cada uno de los sistemas de información de Sociedad de Coberturas serán controladas por medio de la creación de cuentas de usuario a los cuales se les controlarán los privilegios de acceso, modificación y eliminación, de conformidad con los roles y perfiles establecidos.

Controles:

Aprobaciones Requeridas para la Creación de Usuarios y Permisos: Para la creación, actualización o bloqueo de cuentas de usuario a los sistemas de información, las solicitudes para dichas actividades deben contener de forma clara y precisa la siguiente información

1. Nombre completo del funcionario
2. Correo electrónico Para notificación de Contraseñas.

3. Tipo de Permiso (Consulta, Ingreso de información, Actualización de Información, Facturación)
4. Tipo de vinculación: (Personal de Planta o Prestación de Servicios)
5. Si es personal de prestación de servicios, la fecha final del contrato
6. En caso de solicitar acceso a más de un aplicativo se debe especificar por cada uno de ellos los permisos a los que va a tener derecho

Cambio Forzoso de Todas las Contraseñas del Administrador

Siempre que se detecte un ingreso no autorizado al sistema de información, los administradores del sistema deben cambiar inmediatamente cada una de sus contraseñas en el sistema.

Cambios de Contraseñas Periódicas para el Administrador

Todos los administradores deben cambiar periódicamente la contraseña en el sistema.

Control de Acceso al Sistema con Contraseña Individual para cada Usuario

Se precisa que el control de acceso al sistema, se debe realizar por medio de Usuario único, es decir que no se puede tener el acceso a la base de datos y otros recursos del sistema si no se encuentra privilegiado con uno.

Longitud de la Contraseña de Usuario

Se debe tener en la longitud de las contraseñas un mínimo de seis (6) caracteres y una longitud máxima de ocho (8) caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

Confidencialidad de las contraseñas

Se precisa que las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta.

Los empleados serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas.

Cambio de contraseña cuando se sospecha que ha sido descubierta

Ante la posibilidad o sospecha de la perdida de confidencialidad de la contraseña, esta debe ser cambiada de manera inmediata y reportado el evento a la Subgerencia.

Restricción de horarios

Se implementará control de acceso a los aplicativos, en horarios autorizados por los líderes de los procesos propietarios de la información, de tal forma que si se requiere el ingreso en horario adicional al señalado, debe mediar autorización escrita del Gerente, indicando la hora de inicio, finalización y los días que debe estar autorizado.

Cerrar Sesión:
Todos los usuarios deben cerrar sesión cuando no van a hacer más uso del aplicativo, o cuando van a abandonar su estación de trabajo.

Administración de usuarios.
Los Administradores de los sistemas de información, deben revisar con una periodicidad mínima mensual, los derechos de acceso de los usuarios, con el fin de actualizar el estado de los mismos ocasionado por trasladados y retiros de la Entidad.

El uso de programas de acceso remoto será restringido y controlado por la Gerencia, mediante comunicación escrita, especificando el tiempo de utilización, las actuaciones a realizar y la justificación.

Para la instalación y uso de programas de acceso remoto, el usuario autorizado debe garantizar que el acceso remoto se realizará en un equipo seguro, libre de virus, programas maliciosos y espías.

CONTROL DE ACCESO FISICO
Política: El Ingreso al área de servidores y de procesamiento de información será restringido y controlado, y solo se autorizará con fines o propósitos esenciales por Gerente.

Controles:
Toda actividad que se realice por terceros en las áreas de servidores y de procesamiento debe ser supervisada por la Subgerencia.

DISPONIBILIDAD DEL SERVICIO
Política: La Entidad diseñará un plan de contingencia para garantizar la continuidad del servicio de los sistemas de información ante la ocurrencia de eventos inesperados.

Controles
El plan de contingencia de los sistemas de información será diseñado y evaluado semestralmente por la Subgerencia.

La Entidad debe garantizar la disponibilidad de los recursos indicados en el plan de contingencia de los sistemas de información.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La Gerencia y la Subgerencia son responsables de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en Sociedad de Coberturas

8.1 Política y Controles de Organización Interna
La Gerencia y la Subgerencia de Sociedad de Coberturas serán los encargados de tratar los temas concernientes a la seguridad de la información.

8.2 Políticas de Autorización para los Servicios de Procesamiento de Información:
Objetivo: minimizar los riesgos de falla en los sistemas, velar por la utilización adecuada de los recursos y garantizar que estos contribuyan con el cumplimiento de los objetivos institucionales.
Política: La Subgerencia será la responsable de definir y establecer los estándares y procedimientos para el desarrollo, mantenimiento y adquisición de sistemas de información, incluyendo la custodia del código fuente, ambientes de desarrollo, pruebas y producción, y de toda la infraestructura tecnológica relacionada, de conformidad con las mejores prácticas y reglas internacionales de seguridad informática.

Controles de Automatización de Procesos
Desarrollo de Aplicativos
Cualquier solicitud para el Desarrollo de aplicativos nuevos debe tener un proyecto de viabilidad el cual deberá estar debidamente sustentado, una vez sea aprobado por la Gerencia se ordenara iniciar con las fases del ciclo de vida del sistema de información.
Control de Cambios
Al momento que una dependencia requiera alguna modificación, estructural o no, sobre el software aplicativo y si el proceso involucra más de una Dependencia, es necesario que la solicitud de modificación esté autorizada mediante escrito por el Gerente General.

Control de Versiones
La Subgerencia será responsable de gestionar el control de las distintas versiones de desarrollo de un software, de tal forma que se garantice la confidencialidad, integridad y actualización de los documentos.

Publicación de Aplicativos
Para la publicación y puesta en marcha de aplicativos nuevos estos deben estar correctamente diseñados, evaluados de forma minuciosa para evitar la redundancia en las salidas de información.

8.3 Política de Confidencialidad de la Información
Todos los empleados que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes y servicios de telecomunicaciones, personal de

entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por la Entidad, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la información confidencial a la que tengan acceso.

Sociedad de Coberturas identificará la información considerada clasificada o reservada, índice que deberá ser divulgado de conformidad con la normatividad vigente.

Sociedad de Coberturas establecerá controles para el intercambio de información con terceros para asegurar la reserva e integridad de la misma y que se respeten los derechos de autor.

La información clasificada reservada confidencial solo se debe transmitir por medios seguros.

8.4 Política de Seguridad de acuerdos con terceros
Los acuerdos con terceras partes que impliquen acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de la información de Sociedad de Coberturas o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los controles pertinentes a fin de minimizar los riesgos y de mantener la seguridad de la información y de los servicios de procesamiento.

Controles

Sociedad de Coberturas identificará los riesgos para la información y servicios de procesamiento de información que involucran a terceros e implementará los controles adecuados antes de autorizar el acceso.

Sociedad de Coberturas considerará todos los requisitos de seguridad de la información identificados, antes de dar acceso a los activos de información a partes externas.

9. GESTION DE ACTIVOS

9.1 Política de Generación y Restauración Copias de Seguridad.
En Sociedad de Coberturas todo activo de información que sea de interés para un proceso operativo o de misión crítica de la Empresa, deberá ser respaldado con copias de seguridad, con una frecuencia de 15 días calendario.

Controles:
Todos los equipos de cómputo de Sociedad de Coberturas tienen conexión directa con el servidor almacenando la información directamente en este equipo al cual se le hace periódicamente el backup mencionado.

En ningún caso las copias de seguridad serán almacenadas en el mismo equipo donde se encuentra la información.

Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.

El Contratista de Sistemas realizara pruebas de restauración de los backups con la periodicidad establecida en el plan de copias de seguridad, para garantizar que las copias son leídas y restauradas correctamente.

La Subgerencia será la encargada de hacer el backup correspondiente en los tiempos estipulados.

La Gerencia conservará las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las medidas protección y seguridad física adecuadas.

9.2 Política de Archivo de Documentos y Retención de Datos
Política: En Sociedad de Coberturas el archivo de documentos y la retención de datos está debidamente clasificada y controlada por personas a cargo de la Sugerencia y la Gerencia de la compañía.

9.3 Políticas para el Manejo de los Datos
Uso Compartido
Política: El Gerente es quien autoriza el uso compartido de carpetas y por tanto, es responsable por las acciones y el acceso a la carpeta de la información compartida.
Controles
El Gerente debe delimitar a los usuarios que realmente la necesitan y controlar el tiempo en el cual estará expuesta.
La Subgerencia debe asegurarse que el usuario autorizado cuente con el antivirus autorizado.
Antivirus

Política: Todos los equipos de la entidad deben tener instalado, en funcionamiento, actualizado y debidamente licenciado un antivirus, el cual será suministrado por la Gerencia de la Compañía.

Controles:

La Subgerencia es la responsable de controlar las renovaciones de los antivirus según sea la vigencia de estos.

Está prohibido que los empleados de Sociedad de Coberturas desinstalen el antivirus de su equipo, modifiquen o eliminen las configuraciones de seguridad que previenen la propagación de virus, ya que esta acción puede ocasionar riesgo total de contaminación de virus.

Los empleados deben asegurarse que todos los medios de almacenamiento tanto internos como externos están libres de virus o software malicioso, mediante la ejecución del software antivirus autorizado.

Los empleados que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a la Subgerencia para que le brinden el soporte técnico de erradicación del virus.

Todos los archivos anexos a los mensajes recibidos en el correo institucional, estarán sujetos al análisis del antivirus, y el destinatario final recibirá solo los que hayan sido exitosos.

Bases de Datos

Política: El Administrador de bases de datos, no podrá manipular directamente los datos, salvo en circunstancias en las cuales los aplicativos no lo permitan, y solo lo realizará cuando medie autorización escrita del Gerente de la Empresa, y con el debido soporte que requiera de la actualización respectiva.

Controles:

Se deben programar todas las tareas de afinamiento de las bases de datos y los sistemas de información de manera periódica, de acuerdo con la cantidad de solicitudes o quejas de los usuarios respecto de la disponibilidad de las aplicaciones.

El acceso a las bases de datos de los sistemas se realizará de conformidad con las políticas de acceso.

Medios de Almacenamiento Removibles:

Política: Los empleados de Sociedad de Coberturas que contengan información confidencial de propiedad de la Entidad en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Controles:
Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido.

Toda copia de respaldo que se encuentre en medios de almacenamiento removible deberá ser guardada bien sea en caja bajo llave o en un lugar seguro, al cual solo tendrá acceso el responsable de esta.

No está autorizado el uso de los dispositivos de almacenamiento externos removibles que contenga información de la Sociedad de Coberturas, en lugares de acceso público como cibercafés o en equipos que no garanticen la confiabilidad e integridad de la información.

La información de la Empresa clasificada como confidencial que sea transportada en medios de almacenamiento removible, debe ser protegida mediante cifrado o contraseñas, para garantizar que no pueda ser vista por terceros en caso de robo o extravío.

Encadenado de Información entre Documentos y Archivos
Política: Todo documento considerado confidencial debe ser autocontenido y no depender de la disponibilidad e integridad de fuentes externas de datos.

Nombres de Carpetas y Archivos
Política: La identificación de las carpetas y archivos debe ser lógico y de fácil identificación

10. SEGURIDAD DE RECURSOS HUMANOS

10.1 POLÍTICA RELACIONADA CON LA VINCULACIÓN DE COLABORADORES: Sociedad de Coberturas reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos colaboraddores se realizara por medio de un proceso de selección, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

10.2 Normas relacionadas con la vinculación de colaboradores.
La Subgerencia es la responsable de realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en SOCIEDAD DE COBERTURAS, antes de su vinculación definitiva.

Todos los empleados que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes y servicios de telecomunicaciones, personal de entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por la Entidad, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la información confidencial a la que tengan acceso.
Sociedad de Coberturas identificará la información considerada clasificada o reservada, índice que deberá ser divulgado de conformidad con la normatividad vigente.

Sociedad de Coberturas establecerá controles para el intercambio de información con terceros para asegurar la reserva e integridad de la misma y que se respeten los derechos de autor.

La información clasificada reservada confidencial solo se debe transmitir por medios seguros.
Los acuerdos con terceras partes que impliquen acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de la información de Sociedad de Coberturas o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los controles pertinentes a fin de minimizar los riesgos y de mantener la seguridad de la información y de los servicios de procesamiento.

Controles

Sociedad de Coberturas identificará los riesgos para la información y servicios de procesamiento de información que involucran a terceros e implementará los controles adecuados antes de autorizar el acceso.

Sociedad de Coberturas considerará todos los requisitos de seguridad de la información identificados, antes de dar acceso a los activos de información a partes externas.

11. SEGURIDAD FISICA Y AMBIENTAL

SEGURIDAD FISICA Y DEL ENTORNO

Política: Los equipos que hacen parte de la infraestructura tecnológica de Sociedad de Coberturas, tales como servidores, estaciones de trabajo, centro de cableado, aires acondicionados, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

Controles:

Está prohibido fumar, beber o consumir alimentos en las áreas de servidores o cercanas a las estaciones de trabajo.

No está autorizado almacenar material peligroso, combustible e inflamable en sitios cercanos a las áreas de procesamiento o almacenamiento de información.

12. GESTION DE COMUNICACIONES Y OPERACIONES

12.1 Procedimientos y Responsabilidades de Operación
No aplica

12.2 Protección contra Software Malicioso
Política: Toda adquisición de recurso tecnológico en Sociedad de Coberturas, deberá contar con la revisión y aprobación previa de los requerimientos técnicos mínimos definidos, por parte del contratista de sistemas externo.
Política: Sociedad de Coberturas en cabeza del Gerente protegerá la propiedad intelectual propia y de terceros. El software registrado con Derechos de Autor no se podrá copiar sin previa autorización del propietario.
Política: Todo proceso de cambio de Software deberá contar con un plan de contingencia, de tal forma que se garantice la continuidad de los procesos, la salvaguarda e integridad de la información.

Controles:
Adquisición de Equipos de Cómputo: La Subgerencia verificará las características y el estado de todos los equipos digitales y análogos que ingresan a Sociedad de Coberturas. Todos los dispositivos adquiridos deben contar con la garantía de fábrica. Esta debe acreditarse con documento equivalente a certificación o documento expedido por la casa fabricante de cada dispositivo, la cual debe tener el tiempo de garantía, tipo de garantía y tipo de cubrimiento, además el centro autorizado para efectos de la garantía debe estar ubicado en la Ciudad de Bogotá.

Los equipos que hayan sido importados deben contar con el certificado de manifiesto de aduana.

La CPU y los periféricos como son monitor, mouse y teclado que adquiera la Entidad, deben ser de la misma marca. En ese sentido la empresa requiere que tanto los computadores de escritorio y equipos portátiles sean de la misma casa fabricante. Los componentes internos que conforman la CPU deberán ser respaldados por la casa fabricante de los equipos de cómputo.

Cuando los equipos de cómputo e impresoras adquiridas sean de marca de fabricación extranjera, se deberá garantizar que el respaldo de repuestos y suministros en Colombia. Mínimo para cinco (5) años.

Mantenimiento: Los empleados no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos. El empleado que requiera soporte técnico debe dar aviso a la Subgerencia para que contacte al contratista y este a su vez envíe el personal especializado a diagnosticar el equipo.

Responsabilidad de la tenencia: El recurso tecnológico asignado será de uso exclusivo para labores propias de la Entidad y será responsabilidad del usuario que los retire de las instalaciones sin la respectiva autorización de la Subgerencia y registro de la novedad en la planilla elaborada para tal fin.

Los empleados a quienes se les asignen equipos de cómputo portátiles deberán adoptar las medidas de seguridad necesarias que garantizar la seguridad física del recurso tecnológico y salvaguardar la información.

Los empleados deben dar aviso de inmediato a la Subgerencia, de la pérdida o hurto del recurso tecnológico a su cargo, para que se surta el procedimiento establecido.

Los empleados deben comunicar de manera inmediata a la Subgerencia cuando detecte posibles riesgos por factores tales como humedad, inundaciones,choques eléctricos, robo, calentamientos etc.

Los empleados no deben consumir alimentos en áreas cercanas al recurso tecnológico.

La Subgerencia será la responsable de Administrar las hojas de vida del recurso tecnológico, en la cual se registre todos los componentes con sus seriales, el software instalado con su número de licencia respectiva y además el registro de todos los mantenimientos realizados, tanto preventivos como correctivos.

Antivirus
Política: Todos los equipos de la entidad deben tener instalado, en funcionamiento, actualizado y debidamente licenciado un antivirus, el cual será suministrado por la Gerencia de la Compañía.
Controles:
La Subgerencia es la responsable de controlar las renovaciones de los antivirus según sea la vigencia de estos.
Está prohibido que los empleados de Sociedad de Coberturas desinstalen el antivirus de su equipo, modifiquen o eliminen las configuraciones de seguridad que previenen la propagación de virus, ya que esta acción puede ocasionar riesgo total de contaminación de virus.

Los empleados deben asegurarse que todos los medios de almacenamiento tanto internos como externos están libres de virus o software malicioso, mediante la ejecución del software antivirus autorizado.

Los empleados que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a la Subgerencia para que le brinden el soporte técnico de erradicación del virus.

Todos los archivos anexos a los mensajes recibidos en el correo institucional, estarán sujetos al análisis del antivirus, y el destinatario final recibirá solo los que hayan sido exitosos.

12.3 Respaldo o backup

En Sociedad de Coberturas todo activo de información que sea de interés para un proceso operativo o de misión crítica de la Empresa, deberá ser respaldado con copias de seguridad, con una frecuencia de 15 días calendario.

Controles:

Todos los equipos de cómputo de Sociedad de Coberturas tienen conexión directa con el servidor almacenando la información directamente en este equipo al cual se le hace periódicamente el backup mencionado.

En ningún caso las copias de seguridad serán almacenadas en el mismo equipo donde se encuentra la información.

Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.

El Contratista de Sistemas realizara pruebas de restauración de los backups con la periodicidad establecida en el plan de copias de seguridad, para garantizar que las copias son leídas y restauradas correctamente.

La Subgerencia será la encargada de hacer el backup correspondiente en los tiempos estipulados.

La Gerencia conservará las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las medidas protección y seguridad física adecuadas.

12.4 Gestión de Seguridad enla red

Legalidad del Software: Todo software instalado en equipos de la Empresa, será autorizado o instalado por el contratista definido por la Gerencia, la cual tiene autonomía para desinstalar o borrar software no autorizado, en desarrollo de actividades de control de uso de software legal.

Los empleados no deben instalar en los equipos de cómputo de propiedad de Sociedad de Coberturas ningún tipo de Software.

El empleado asumirá la responsabilidad por el software instalado en el computador que le sea asignado o que esté utilizando. Toda aplicación que esté instalada debe estar

debidamente licenciada.

Sistemas Operativos:
Los equipos servidores o los que hagan sus veces, deben contar con el software para realizar el chequeo de integridad del sistema operativo y del hardware.

USO DE SERVIDORES
Política: El Subgerente es el responsable de verificar la instalación y configuración de todo servidor que sea conectado a la red, y de implementar mecanismos de seguridad física y lógica.
Controles:
Ubicación de Servidores: Los servidores estarán ubicados en un área física que cumpla con las siguientes medidas de seguridad:
· El acceso debe ser restringido a personal autorizado
· La temperatura debe ser la adecuada para la cantidad de equipos
· Debe tener protección contra descargas eléctricas
· El mobiliario debe ser el adecuado
· Ubicación física en sitio libre de daño por humedad, goteras, inundaciones y demás efectos del clima.

Funcionalidad y mantenimiento de Servidores: Todo servidor que proporcione servicios a través de la red debe:
· Funcionar las 24 horas al día los 365 días del año
· Tener mantenimiento preventivo mínimo dos veces al año
· Ser objeto de Mantenimiento semestral donde se realizara la depuración de bitácoras
· Hacerle revisión de su configuración anual
· Ser Monitoreado diariamente por el Subgerente.

12.5 Gestión de medios
Política: En Sociedad de Coberturas el archivo de documentos y la retención de datos está debidamente clasificada y controlada por personas a cargo de la Sugerencia y la Gerencia de la compañía.

12.6 Intercambio de Información
Uso Compartido
Política: El Gerente es quien autoriza el uso compartido de carpetas y por tanto, es responsable por las acciones y el acceso a la carpeta de la información compartida.
Controles
El Gerente debe delimitar a los usuarios que realmente la necesitan y controlar el tiempo en el cual estará expuesta.
La Subgerencia debe asegurarse que el usuario autorizado cuente con el antivirus autorizado.

Bases de Datos
Política: El Administrador de bases de datos, no podrá manipular directamente los datos, salvo en circunstancias en las cuales los aplicativos no lo permitan, y solo lo realizará cuando medie autorización escrita del Gerente de la Empresa, y con el debido soporte que requiera de la actualización respectiva.

Controles:
Se deben programar todas las tareas de afinamiento de las bases de datos y los sistemas de información de manera periódica, de acuerdo con la cantidad de solicitudes o quejas de los usuarios respecto de la disponibilidad de las aplicaciones.

El acceso a las bases de datos de los sistemas se realizará de conformidad con las políticas de acceso.

Medios de Almacenamiento Removibles:
Política: Los empleados de Sociedad de Coberturas que contengan información confidencial de propiedad de la Entidad en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Controles:
Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido.

Toda copia de respaldo que se encuentre en medios de almacenamiento removible deberá ser guardada bien sea en caja bajo llave o en un lugar seguro, al cual solo tendrá acceso el responsable de esta.

No está autorizado el uso de los dispositivos de almacenamiento externos removibles que contenga información de la Sociedad de Coberturas, en lugares de acceso público como cibercafés o en equipos que no garanticen la confiabilidad e integridad de la información.

La información de la Empresa clasificada como confidencial que sea transportada en medios de almacenamiento removible, debe ser protegida mediante cifrado o contraseñas, para garantizar que no pueda ser vista por terceros en caso de robo o extravío.

Encadenado de Información entre Documentos y Archivos
Política: Todo documento considerado confidencial debe ser autocontenido y no depender de la disponibilidad e integridad de fuentes externas de datos.
Nombres de Carpetas y Archivos
Política: La identificación de las carpetas y archivos debe ser lógico y de fácil

identificación.

USO DEL CORREO ELECTRONICO

Política: El Gerente es el encargado de definir los nombres, estructura y plataforma que se debe utilizar para la cuenta de correo Institucional de cada funcionario.

Controles:

Administración del Correo Institucional: El uso del correo institucional es de carácter corporativo, siendo responsabilidad de la Gerencia el control de este. La Gerencia podrá delegar en la Subgerencia por escrito esta función de la administración del correo.

El tamaño del buzón, de los archivos enviados y del contenido del correo será definido por la Subgerencia.

Cambio de Contraseñas a Correos Institucionales: Los cambios de contraseñas solo podrán ser realizados por la Subgerencia de la compañía y solo serán de conocimiento del funcionario que tenga las funciones específicas. En caso de cambio de funcionario la Subgerencia deberá, de forma inmediata realizar el cambio en las contraseñas.

Envíos y Transferencias en Correos Institucionales: Todo correo institucional debe ser descargado periódicamente de la bandeja de entrada para así liberar y dar capacidad al servidor, garantizando la seguridad de la información.

Copias de seguridad de los correos institucionales: Las copias de seguridad de los correos institucionales se harán en conjunto con el backup quincenal establecido para la compañía.

Recepción e Intercambio de información: El intercambio de información entre Sociedad de Coberturas y terceros a través de correos electrónicos, se hará única y exclusivamente por medio de los correos institucionales, y en ningún caso por medio de correos personales.

El usuario responsable del correo institucional debe evitar abrir los adjuntos de correos de origen desconocido o que contengan palabras en Ingles a fin de evitar los virus, a menos que haya sido analizado previamente por el antivirus autorizado.

El correo institucional será de uso exclusivo para fines propios de la Sociedad de Cobertura y en su uso se dará aplicación al código de ética; En consecuencia es prohibido utilizar el correo institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de los personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

Los usuarios del correo institucional deben evitar enviar respuestas a todos los

destinatarios del correo inicial, salvo en los casos que sea absolutamente necesario, sobre todo en los casos en los cuales el correo original fue enviado de manera masiva.

12.7 Monitoreo
No aplica.

13. CONTROL DE ACCESO

13.1 Requerimiento para el Control de Acceso
Sociedad de Coberturas establecerá privilegios para el control de acceso de los colaboradores a sus equipos. Así mismo, velará porque los colaboradores tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

13.2 Gestión de Acceso del Usuario
No aplica.

13.3 Responsabilidades del Usuario
Los usuarios de los recursos tecnológicos y los sistemas de información Sociedad de Coberturas realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

13.4 Control de Acceso a la Red
Los colaboradores de Sociedad de Coberturas deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos. Los colaboradores no deben compartir sus cuentas de usuario y contraseñas con otros colaboradores.

13.5 Control de Acceso al Sistema Operativo
Sociedad de Coberturas, como propietaria de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. La Subgerencia, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

13.6 Control de Acceso a las Aplicaciones y la Informaicón
Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos. Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

14.1 Requerimientos de Seguridad de los sistemas de información
Sociedad de Coberturas establecerá, a través de Subgerencia, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la empresa.

14.2 Controls Criptográficos
Sociedad de Coberturas velará porque la información de la empresa, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

14.3 Seguridad en los procesode de desarrollo y soporte
No aplica.

14.4 Gestión de la vulnerabilidad técnica

Sociedad de Coberturas, a través de la Subgerencia, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

15. GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION

Sociedad de Coberturas promoverá entre los empleados el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como el servidor, los sistemas de información, los medios físicos de almacenamiento y las personas. De igual manera, asigna a la Subgerencia para el tratamiento de los incidentes de seguridad de la información, quien tendrá la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad. La Gerencia es la única autorizada para reportar incidentes de seguridad ante las autoridades.

Es responsabilidad de los empleados de Sociedad de Coberturas reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible. En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los empleados deben notificarlo a la Subgerencia para que se registre y se le dé el trámite necesario.

16. CUMPLIMIENTO

Sociedad de Coberturas velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

17. REGISTROS DE REFERENCIA

Las políticas de seguridad han sido formuladas teniendo como referencia la Norma NTCISO/ IEC 27001.

Fecha: 21 de septiembre de 2018

Elaboró:

NIDIA AIDÉ GONZÁLEZ PÁEZ
Subgerente

Aprobó

EDWIN VILLEGAS BOTERO
Gerente