OBJETIVOS DE LA POLÍTICA

El objetivo de la Política de Seguridad de la información consiste en establecer unos criterios, directrices y estrategias que le permitan a SERVERS & SOFTWARE S.A.S y de sus clientes, proteger su información, así como la tecnología y el control de la misma en el procesamiento, administración, manipulación de los datos e información.

La Política de Seguridad de la información proporciona la base para la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades en los sistemas y centro de datos.

El propósito de estructurar Políticas de Seguridad de la información es, por tanto, garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno y las tecnologías.

Este documento formaliza el compromiso de la Alta Dirección frente a la gestión de la seguridad de la información y presenta de forma escrita a los usuarios de sistemas de información el compendio de acciones con las cuales Servers & Software S.A.S., establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos, los cuales están en constante cambio y evolución de acuerdo con el avance tecnológico y los requerimientos de los clientes.

1. MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Todos los procedimientos que figuran en este documento están aprobados, apoyados y respaldados por la Alta Dirección de SERVERS & SOFTWARE S.A.S.
Para la Organización está claro que los datos depositados en los sistemas informativos deben ser protegidos de acuerdo con su criticidad, valor y sensibilidad de la misma.

Las medidas de seguridad de la información deben ser tomadas, independientemente de los medios de almacenamiento, los sistemas utilizados para procesarla o los métodos usados para la transferencia de la misma.

2. ALCANCE

El alcance de esta política es proteger y salvaguardar todos los sistemas informáticos, sistemas de envió, de almacenamiento de información, medio de información clasificada, o centro de datos. Con el fin de prevenir incidentes y perdidas de información dando un alcance de a nivel Corporativo de manera que todos los empleados se

someten a la validación, uso, y cumplimiento. De las normas comprendidas dentro del plan de seguridad de la información. Establecidos por el área de sistemas y la alta gerencia.

3. DEFINICIONES

Para efectos del presente documento se entiende por:

Análisis de Riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Amenaza: Es un evento que puede desencadenar un incidente en el sistema informático, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: Evento, exitoso o no que atenta sobre el buen funcionamiento del Sistema Informático.

Buzón: También conocido como Cuenta de correo electrónico o de E-Mails.

Confidencialidad: Es asegurar que la información es accesada sólo por las personas autorizadas para ello.

Contraseña o Clave (Password): Es una forma de autenticación o control de acceso que utiliza información secreta para controlar el acceso hacia algún recurso informático. Puede está conformado por números, letras y/o caracteres especiales.

Disponibilidad: Es asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando éstos sean requeridos.

Dispositivos USB: Es un dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir y no necesita baterías (pilas).

Evaluación de Riesgos: Todo proceso de análisis y valoración del riesgo.

FTP: (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos): En informática es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Información confidencial (RESERVADA): Información administrada por Servers & Software S.A.S., en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida con previa autorización del titular de la misma.

Información confidencial (CONFIDENCIAL): Información generada por La Servers & Software S.A.S., en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso del titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

Información privada (USO INTERNO): Información generada por La Servers & Software S.A.S., en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

Información pública: Es la información administrada por Servers & Software S.A.S., en cumplimiento de sus deberes y funciones que está a disposición del público en general; por ejemplo, la información de los registros públicos y la información vinculada al Registro Único Empresarial y Social – RUES.

Impacto: Medición de los efectos que se generan en el Sistema Informático cuando se materializa una amenaza.

Incidente de Seguridad de la información: Es un evento atribuible a una causa de origen humano. Esta distinción es particularmente importante cuando el evento es el producto de una intención dolosa de hacer daño. Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Integridad: Mantenimiento de la exactitud e integralidad de la información y sus métodos de proceso.

Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Plan de Contingencia: Disponibilidad de recursos para atender oportunamente una eventualidad en el Sistema Informático.

Política de Seguridad de la información: Consiste en asegurar que los recursos y la información soportada en la plataforma informática (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. Toda intención y directriz expresada formalmente por la alta dirección.

Red Privada Virtual o VPN (siglas en inglés de Virtual Private Network): Es una tecnología de red que permite una extensión de la red local sobre una red pública.

Riesgo: Es la probabilidad de ocurrencia de un hecho favorable o desfavorable que pudiera afectar la Seguridad de la información.

Sistema de Información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo).

Sistema Multiusuario: Se refiere a un concepto de sistemas operativos, pero en ocasiones también puede aplicarse a programas de ordenador de otro tipo (e.j. aplicaciones de base de datos). En general se le llama Multiusuario a la característica de un Sistema Operativo o Programa que permite proveer servicio y procesamiento a múltiples usuarios simultáneamente.

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un Sistema Informático.

Software Malicioso: Programa o parte de un programa destinado a perturbar, alterar o destruir la totalidad o parte de los elementos de la lógica esencial para el funcionamiento de un sistema de procesamiento de la información. Estos programas se pueden dividir en cuatro clases: los virus informáticos, gusanos, troyanos y bombas lógicas.

Unidad Central de Procesamiento o CPU: Es el componente en un ordenador o computador que interpreta las instrucciones y procesa los datos contenidos en los programas de la computadora.

Valoración del riesgo: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

Virus: Es un programa de ordenador que puede copiarse a sí mismo e infectar un ordenador.

Vulnerabilidad: Son aspectos que influyen negativamente en la Seguridad de la información y que posibilitan la materialización de una amenaza.

4. ROLES Y RESPONSABILIDADES

4.1. Direcciones o Áreas responsables de la Seguridad de la información

El Comité de Seguridad de la información, conformado por la Alta Dirección y el líder de ingeniería, Son los responsables de establecer y mantener las Políticas de Seguridad de la información, las normas, directrices y procedimientos de la Organización. Alineados a la legislación aplicable.

Las siguientes son las principales responsabilidades a cargo del Comité de Seguridad de la información, dentro de la Entidad:

- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la organización.
- Revisión y valoración de la Política de Seguridad de la información.
- Alineación e integración de la seguridad a los objetivos del negocio.
- Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.
- Establecer las funciones y responsabilidades específicas de seguridad de la información para Servers & Software S.A.S
- Verificar, a través de reuniones semestrales, el estado de la seguridad y protección de la información en SERVERS & SOFTWARE S.A.S y la necesidad de nuevos proyectos y actualizaciones en temas de seguridad.
- Establecer y respaldar los programas de concientización de SERVERS & SOFTWARE S.A.S en materia de seguridad y protección de la información.
- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información
- Evaluar los controles de seguridad específicos para nuevos servicios o sistemas de información.
- Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización y partes interesadas.

- Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización. Revisar y seguir los incidentes de seguridad de la información.

La investigación de incidentes de Seguridad de la información es responsabilidad del Líder del área de Ingeniería.

Las medidas disciplinarias en respuesta a las violaciones de las normas de Seguridad de la información se adoptarán de acuerdo con los lineamientos establecidos en el Reglamento Interno de Trabajo de la SERVERS & SOFTWARE S.A.S., estableciendo como una falta grave.

4.2. **Responsabilidades del Empleado**

Los empleados deben tomar conciencia de la importancia del establecimiento de la Política de Seguridad de la información, los procedimientos y la normatividad aplicable. Estas normas deben ser completamente entendidas y aplicadas en la cotidianidad de sus tareas.

Los empleados que sean responsables de la información deben establecer los medios que soporten la toma de decisiones con base en la información que se encuentre a su cargo.

Los empleados que sean responsables de la información deben establecer la clasificación que mejor refleje el carácter sensible, el valor crítico y la disponibilidad de cada tipo de información que se encuentre bajo su cuidado. Esta clasificación determinará el nivel de acceso a los empleados.

Los empleados, además de ser responsables de la información, serán también los encargados de administrarla. En consonancia con lo anterior serán responsables todos aquellos que manejen información en los computadores asignados para llevar a cabo sus actividades o que tengan acceso a cualquier aplicación o sistema que sirva de apoyo a sus tareas.

Son responsables por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que otra persona realice labores bajo su identidad. De forma similar, los empleados y usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o

negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de SERVERS o de la propiedad de los clientes.

Los empleados responsables de la información deberán almacenarla, implementar los controles de acceso (para prevenir la divulgación no autorizada) y periódicamente hacer copias de respaldo y así evitar la pérdida de información crítica.

4.3. **Declaración de reserva de derechos de SERVERS & SOFTWARE S.A.**S

Servers & Software S.A.S. usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información.

Para mantener estos objetivos Servers & Software S.A.S., se reserva el derecho y la autoridad de:

5. Restringir o revocar los privilegios de cualquier usuario.
6. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en

contra de los objetivos antes planteados.

7. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de Servers & Software S.A.S. o de sus clientes.

Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del comité de seguridad siempre con el concurso de la alta dirección o de quién él delegue esta función.

6. SENSIBILIDAD Y CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información constituye un elemento importante para la administración del riesgo, ya que determina la prioridad y el grado de protección requerido para cada tipo de información que repose en los sistemas informáticos.

Servers & Software S.A.S., ha definido unos criterios para la clasificación de la información que reposa en la plataforma informática. Estos criterios establecen el nivel apropiado de protección para cada una de las categorías e informa a los empleados responsables de cualquier medida especial o tratamiento requerido. Toda la información del Sistema Informático debe estar clasificada dentro de los siguientes criterios:

- ✓ **Confidencial**: Hace referencia a aquella información que solamente puede ser conocida y manejada por personal expresamente autorizado para su uso y/o atender solicitudes derivadas de los procesos de auditorías internas o externas y/o para atender requerimientos de orden legal o jurídico.
- ✓ **De Uso Interno**: Información que puede ser de libre utilización por los empleados de Servers & Software para llevar a cabo las actividades laborales. EI acceso a esta información está restringido a los miembros de cada área o disponibles para los ejercicios de auditoría interna o externa de la compañía.

- ✓ **Pública**: Es aquella información que podrá ser utilizada o conocida por todos los empleados de Servers & Software e, incluso, por terceros.

Para garantizar la Seguridad de la información todos los empleados deben familiarizarse con la definición de cada categoría, así como también con las medidas aplicadas.

6.1. SEGURIDAD INFORMATICA

- ✓ **Acceso de información por parte de Terceros**

El acceso a terceros de la información de la Organización será permitido siempre y cuando haya la debida autorización previa del jefe del Área responsable de la misma.
Cuando el suministro de la información involucre aspectos tecnológicos deberá contarse adicionalmente con el visto bueno previo del Líder de Ingeniería, quien deberá validar los riesgos de la seguridad de la información requerida, por canales de comunicación seguras.

- ✓ **Requerimiento de información por parte de terceros**

Las solicitudes de información registral, informes financieros, documentos de políticas internas, actas, manuales, estudios económicos, procedimientos, y, en general, todo tipo de información, se encuentran amparados y dando cumplimiento a los lineamientos de la Política de Seguridad de la Información.

- ✓ **Divulgación de la seguridad de la información a personal externo**

La información relativa a las medidas de seguridad, a los sistemas de procesamiento de información y a las redes es confidencial y no debe ser divulgada a usuarios no autorizados a menos que se cuente con la autorización del Líder de ingeniería.

6.2. CONTROLES PARA LA ADMINISTRACIÓN DE LA SEGURIDAD

Los empleados deberán ser informados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes.

- ✓ **Uso de los recursos tecnológicos de la organización**

Todos los empleados que utilicen los sistemas de procesamiento de la información o los recursos de SERVERS & SOFTWARE S.A.S, deberán actuar basados en las normas establecidas en la Política de Seguridad de la información.

Los sistemas de información de Servers & Software S.A.S., deberán ser utilizados exclusivamente con fines Organizacionales.

El uso con fines personales de los recursos tecnológicos de Servers & Software S.A.S., está permitido siempre y cuando sea en tiempo no laboral y no afecte la productividad ni la seguridad de la información corporativa.

Se prohíbe la utilización de los computadores y recursos de Servers & Software S.A.S., para ejecutar juegos de cualquier índole. Estas actividades darán lugar a acciones disciplinarias.

- ✓ **Derechos de Vigilancia**

El Líder de Ingenieria-mesa de ayuda, previa autorización de la Dirección, se reservará el derecho de supervisar, monitorear e inspeccionar en cualquier momento los sistemas de información utilizados por los empleados y que sean de propiedad de la compañía. Las inspecciones pueden llevarse a cabo con o sin el consentimiento y presencia del empleado involucrado.

Los Sistemas de Información sujetos a dicha inspección incluyen los registros de la actividad de los empleados: archivos y correos electrónicos institucionales y soportes físicos de la información auditada pueden ser sujetos de la misma inspección en cualquier momento. Lo anterior, sin perjuicio del respeto a la intimidad personal y a la inviolabilidad de la correspondencia y demás formas de comunicación privada en los términos del mandato constitucional.

- ✓ **Declaración de propiedad Exclusiva**

SERVERS & SOFTWARE S.A.S tiene propiedad y derechos exclusivos sobre las patentes, derechos de autor, invenciones, programas o cualquier otra propiedad intelectual desarrollada por sus empleados en la plataforma tecnológica de la entidad.

- ✓ **Acceso a Internet**

Todos los empleados con sistemas de información asignados tendrán acceso a Internet desde sus estaciones de trabajo. Servers & Software S.A.S., se reserva el derecho de retirar o restringir dicho acceso.

El acceso a Internet será monitoreado por el área de Ingeniería, para asegurar el uso apropiado y el cumplimiento de las Políticas de Seguridad.

SERVERS & SOFTWARE S.A.S dispone de un software para el control de la navegación en Internet, el cual restringe el acceso a las categorías que universalmente las instituciones bloquean como por ejemplo sitios de contenido pornográfico, consumo de ancho de banda, contenidos racistas, violencia, ocio, etc. Dicho software genera periódicamente los informes de los resultados (logs) de la navegación, los cuales quedan disponibles respectivo análisis y seguimiento de dicho informe de ser requeridos por los líderes de áreas que los requiera. De necesitarse el acceso a una página bloqueada deberá ser autorizado por el líder/coordinador del área de ingeniería – mesa de ayuda.

El acceso a Internet debe ser utilizado para las actividades relacionadas con las necesidades del puesto y función que desempeña.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por SERVERS. En caso de necesitar una conexión especial a Internet, ésta tiene que ser notificada y aprobada por el Líder de Ingenieria.

Los empleados de SERVERS & SOFTWARE S.A.S con acceso a Internet tienen que reportar todos los incidentes de seguridad de la información Ingeniería; inmediatamente después de su identificación.

El uso de módem para acceso a Internet está prohibido, en caso de requerir su uso, debe ser previamente autorizado por el Líder de Ingenieria.

Se prohíbe el uso de aplicaciones, programas y/o herramientas que saturen los canales de comunicación o Internet, tales como gestores de descarga de archivos multimedia, con excepción de los autorizados por líderes de área.

Los empleados de SERVERS & SOFTWARE S.A.S con acceso a Internet, al acceder al servicio están aceptando que:

1. Serán sujetos de monitoreo de las actividades que realizan en Internet.

2. Existe la prohibición de acceso a páginas no autorizadas.
3. Se prohíbe la transmisión de archivos reservados o confidenciales no autorizados.
4. Se prohíbe la descarga de software sin la autorización del área de Ingeniería.
5. La utilización de Internet es para el desempeño de su función en SERVERS y no para propósitos personales.

SERVERS & SOFTWARE S.A.S ofrece un correo electrónico y servicios de mensajería electrónica para facilitar la ejecución de sus actividades.

El intercambio de correos debe utilizar los buzones institucionales. Está prohibido tramitar información institucional a través de e-mails privados o de uso personal.

El tamaño para los contenidos de los archivos adjuntos enviados por email no podrá exceder 15 Mb (megas); de presentarse casos que exceden esta capacidad deberá ser autorizado por el jefe del Área respectiva con el visto bueno del Líder de Ingenieria. Es decir, por defecto, no podrá enviarse un email o correo electrónico cuya sumatoria de los tamaños de los archivos adjuntos del mismo exceda los 10 Mb (Megas), salvo que la necesidad inmediata y puntual así lo requiera.

Los envíos masivos de emails, es decir, envíos masivos a más de 20 remitentes, deberán hacerse utilizando la herramienta instalada o adquirida en la institución, es decir, debereran enviarse a través del software de envío masivo de emails. En ningún caso podrán enviarse emails masivos (más de 20 remitentes) a través de los computadores personales utilizando los clientes de correo.

La firma electrónica establecida para los emails deberá informar: El nombre de la Organización, el cargo del empleado que envía el email, el teléfono y extensión. El tamaño y tipo de fuente utilizada para la misma será de EXO 10.

Se prohíbe el uso del correo electrónico con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son de solo texto, audio, video o una combinación de los tres.

Software e información sensible de SERVERS que requiera ser enviado por Internet debe transmitirse con la mayor seguridad posible acordada entre las partes.

Si fuera necesario leer el correo de alguien más (mientras un empleado se encuentre fuera o de vacaciones) el jefe de la respectiva área determinará a qué buzón deben ser redireccionados sus correos en su ausencia.

Los empleados deben tratar los mensajes de correo electrónico y archivos adjuntos que reciba a través del correo institucional como información de propiedad de SERVERS & SOFTWARE S.A.S

La asignación de una cuenta de correo electrónico de un dominio no institucional externo deberá solicitarse por la plataforma de HELPDESK al Líder de Ingenieria, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Jefe Inmediato.

Está prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Está prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

6.3. COPIA DE RESPALDO Y RESTAURACIÓN

El personal es el encargado de realizar el almacenamiento de información mas relevante perteneciente a su cargo, en la nube de Servers ya prevista por el área de Ingeniería, en pro salvaguardar la información por eventualidades físicas o externas en los equipos.

Ingeniería es la responsable de respaldar la información contenida en la infraestructura de datos de SERVERS, calificados como NIVEL CRITICO, velando por la seguridad y resguardo de los datos contenidos en ellos; así como por su integridad, disponibilidad y confidencialidad.

El área de ingeniería será el responsable de definir los mecanismos adecuados para la ejecución de los respaldos de información, asi como la periodicidad, lugar de archivo y el tiempo de retención de las copias.

La ejecución de las copias de seguridad debe llevarse a cabo en horas de poca o ninguna actividad laboral; por lo tanto, es importante que el responsable defina el horario de ejecución de estas.

En los casos en que el backup no finalice exitosamente dentro de los tiempos establecidos, la plataforma automáticamente enviara un notificación virtual al correo de mesa de ayuda, donde ingeniería relanzara la tarea, en los tiempos establecidos en el procedimiento de Copias de Respaldo.

Cuando el cliente interno o externo requiera un respaldo por demanda de los servidores, se debe solicitar formalmente al correo mesadeayuda@servsoft.com.co, por parte del personal autorizado, para informar mínimo con 24 horas de antelación sobre posibles interrupciones en el servicio a las personas afectadas, estos tiempos pueden ser modificados de acuerdo a la criticidad.

Todos los respaldos se revisarán con la periodicidad definida en el backups y se evidenciarán en la programación de backups.

La Comprobación periódica del estado de las copias se llevará a cabo con el fin de garantizar la disponibilidad e integridad de los datos almacenados.

Los equipos para el respaldo de información de la compañía deben estar ubicados en el Datacenter Central De Datos con las medidas de seguridad pertinentes, y tener el personal de soporte y mantenimiento bajo la regulación vigente.

Los medios de almacenamiento de datos deben tener un manejo adecuado para mitigar la ocurrencia de datos físicos y por consiguiente la perdida de información, sus condiciones mininas deben ser encriptadas.

Servers & Software cuenta con una **"Matriz de Riesgos**", documento que relaciona los diferentes riesgos que pueden ocurrir y las acciones para mitigar o eliminar los riesgos.

6.4. MANEJO DE CAMBIOS

Los cambios en los recursos tecnológicos dispuestos por Servers & Software S.A.S., para llevar a cabo las diferentes actividades deben estar soportados por una solicitud formal, la cual debe relacionarse y justificarse vía caso en el GLPI, cambios que deben ser aprobados por el Jefe de Área del usuario que solicita el cambio y por el Líder de Ingeniería.

El procedimiento para el manejo de cambios se aplicará siempre que se lleve a cabo una modificación importante en los recursos tecnológicos.

Esta Política aplica para todos los elementos que forman parte de la plataforma tecnológica dispuesta por SERVERS & SOFTWARE S.A.S.

6.5. ESTÁNDAR PARA EL DESARROLLO DE SISTEMAS

El desarrollo o mantenimiento de software por parte del personal interno debe tener la aprobación del Líder de Ingeniería, y debe ceñirse a las políticas, estándares, procedimientos y convenciones establecidas por la Organización. Las convenciones o políticas incluyen pruebas, entrenamiento y documentación.

Todo sistema o aplicativo debe contar con ambiente de desarrollo y ambiente de producción. Así mismo para la realización de pruebas no se deben utilizar datos de producción.

- ✓ Cumplimiento del procedimiento para cambios y/o actualizaciones. Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, serán evaluados en ambientes de prueba cuya función es determinar el correcto funcionamiento y compatibilidad con las herramientas base; luego de ello, se debe crear un plan de trabajo para la migración del ambiente de producción a la nueva versión.

- ✓ Documentación de cambios y/o actualizaciones. Todo cambio y/o actualización en los sistemas de información que se encuentren en producción, debe tener la documentación respectiva.

- ✓ Se requieren registros de auditoria en sistemas que manejan información sensible. Todo sistema que maneje información sensible para SERVERS & SOFTWARE S.A.S debe generar registros de auditoria que guarden toda modificación, adición y eliminación de dicha información.

- ✓ Los registros del sistema deben incluir eventos relevantes para la seguridad. Los sistemas de computación que manejan información sensible deben registrar todos los eventos de seguridad relevantes. Ejemplos de eventos de seguridad relevantes son: intentos de intentos de fuerza bruta a las contraseñas, intentos de escalamiento de privilegios no otorgados, modificaciones a la aplicación y modificaciones al sistema.

6.6. MANEJO DE LICENCIAS

Únicamente se autoriza la instalación de software que se encuentre soportado con su respectiva licencia. La adquisición de software será autorizada por la gerencia y supervisada por el área de Ingeniería.

No se permite descargar, instalar o utilizar programas de software no autorizadas. Esta práctica, podría introducir serias vulnerabilidades de seguridad en las redes, sistemas e información de la organización, además de afectar el funcionamiento de su computador. Los paquetes de software que permiten que el equipo sea manejado "a control remoto (por ejemplo, PC anywhere) y "hacking tools" (por ejemplo, sniffers de red y crackers de contraseñas) están explícitamente prohibidas en SERVERS & SOFTWARE S.A.S, a menos que hayan sido expresamente autorizados previamente por la gerencia y aprobados por el Líder de Ingenieria – mesa de ayuda.

Respecto a las licencias de software. La mayoría del software, a menos que esté específicamente identificado como "freeware" o "software de dominio público", sólo puede ser instalado y / o utilizarse si ha sido validado por el Área de Ingeniería. Paquetes de shareware o de prueba deben ser eliminados una vez haya expirado el período de prueba. Algunos programas de software son sólo para uso libre de los particulares, mientras que el uso comercial o empresarial requiere un pago de licencia.

SERVERS & SOFTWARE S.A.S no permite materiales inapropiados, como los archivos pornográficos, racistas, difamatorios o de acoso, fotos, videos o mensajes de correo electrónico que pueda causar ofensa o vergüenza. No está permitido almacenar, usar, copiar o distribuir este material en los computadores de la organización.

El Área de Ingeniería podrá en cualquier momento validar que el software instalado en un computador se encuentre legalmente soportado con su respectiva licencia. De dicha inspección se pasará un reporte al Comité de Seguridad de la información con el fin de informar la relación, el estado y legalidad del software instalado.

El Área de Ingeniería determinará la conveniencia o no de la instalación de un determinado software en un computador.

Los empleados que requieran la instalación de software que no sea propiedad de la SERVERS & SOFTWARE S.A.S deberán justificar su uso y solicitar su autorización al Líder de Ingeniería, indicando el equipo de cómputo donde se instalará el software, el propósito y el período de tiempo que permanecerá dicha instalación, además de respaldar el mencionado software con la respectiva licencia de legalidad.

Las licencias deben ser custodiadas y controladas por el Área de Ingeniería. Esta área debe realizar auditorías de licencia de software como mínimo una vez al año generando las videncias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado el software legal y autorizado por el jefe de cada área.

Se considera una falta grave que los empleados instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de SERVERS & SOFTWARE S.A.S, que no esté autorizado por el jefe del Área respectiva y el Líder de Ingenieria-mesa de ayuda.

7. CONTROLES FÍSICOS AMBIENTALES

7.1. CONTROL DE ACCESO A LA INFORMACIÓN

- ✓ El acceso al centro de cómputo, servidores y áreas de trabajo que contengan información sensible o crítica, como la contenida en los servidores, está restringido y solamente el personal autorizado podrá acceder a estos lugares.

- ✓ La información sensible o crítica debe estar siempre protegida contra la divulgación no autorizada.

- ✓ Documentos impresos que contengan información sensible o crítica deben estar siempre almacenados o guardados en lugares que garanticen su seguridad y conservación y protejan su acceso inclusive durante horas no laborales.

- ✓ El empleado tiene la obligación de proteger los discos, cintas magnéticas, CD-ROM y otros medios de almacenamiento como memorias USB que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

- ✓ Es responsabilidad del empleado evitar en todo momento la fuga de la información de SERVERS & SOFTWARE S.A.S que se encuentre almacenada en los equipos de cómputo personal que tenga asignados

- ✓ Cualquier persona que tenga acceso a las instalaciones de SERVERS & SOFTWARE S.A.S deberá registrar al momento de su entrada el equipo de cómputo, medios de almacenamiento y herramientas que no sean propiedad de la misma, el cual podrán retirar el mismo día.

- ✓ Las computadoras personales, las computadoras portátiles, módems, y cualquier activo de tecnología de información de la entidad sólo podrá ser retirado de las instalaciones con la autorización de salida del área Administrativa y Financiera.

- ✓ Los empleados no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización respectiva. En caso de requerir este servicio deberá solicitarlo a la jefatura Administrativa y Financiera.

- ✓ La Jefatura Administrativa y Financiera será la encargada de generar el resguardo y recabar la firma del empleado como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por

el Área de Ingeniería. El movimiento o retiro de equipos por traslado, reemplazo o baja debe ser informado a la jefatura Administrativa y Financiera, por el Área de Ingeniería y el empleado responsable del activo.

- ✓ El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones de SERVERS & SOFTWARE S.A.S., y los responsables de dichos equipos deberán velar por su adecuado uso, cuidado, mantenimiento y protección

- ✓ Será responsabilidad del empleado solicitar al Área de Ingeniería la asesoría necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- ✓ Se prohíbe conectar a los perfiles de red Corporativos los dispositivos móviles de uso personal, salvo que exista autorización explícita emitida por los jefes de área

- ✓ Es responsabilidad de los empleados almacenar su información únicamente en la partición de disco duro identificada como "Mis Documentos" o similares, ya que es exclusivamente desde ahí donde se generan las copias automáticas de seguridad.

- ✓ Mientras se opera el equipo de cómputo no se deberán consumir alimentos o ingerir líquidos.

- ✓ Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o de la CPU.

- ✓ Se debe mantener el computador en un entorno limpio y sin humedad.

- ✓ El empleado debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

- ✓ Queda prohibido que el usuario abra o desarme los equipos de cómputo. Únicamente el personal autorizado por el Área de Ingeniería podrá llevar a cabo los servicios y reparaciones al equipo de cómputo, por lo que los empleados deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

- ✓ Los empleados y el Área de Ingeniería, deberán asegurarse de respaldar la información que consideren relevante y borrarla cuando el equipo de cómputo sea enviado a reparación, evitando así la pérdida involuntaria de información, derivada del proceso de reparación.

- ✓ El empleado que tenga bajo su custodia algún equipo de cómputo, será responsable de su uso y conservación; en consecuencia, responderá con su propio patrimonio por la pérdida, daño o deterioro que ocurra a los equipos cuando el hecho acontezca por negligencia o culpa del trabajador.

- ✓ El resguardo para los portátiles tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

- ✓ El empleado deberá dar aviso inmediato de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo a la jefatura Administrativa y Financiera.

- ✓ El empleado que tenga bajo su resguardo dispositivos especiales es responsable del buen uso que se les dé.

- ✓ Si algún área por requerimiento muy específico tiene la necesidad de contar con un dispositivo especial o específico, su instalación deberá ser autorizada por la Gerencia con el apoyo del Área de Ingeniería.

- ✓ Deberá configurarse el computador de tal manera que durante un tiempo de inactividad éste sea bloqueado automáticamente y se requiera para el reinicio de actividades el ingreso de una clave, el tiempo de inactividad se ha establecido en 5 minutos.

- ✓ Datos sensibles enviados a través de redes externas deben estar encriptados. Si se ha de transmitir datos sensibles a través de cualquier canal de comunicación externo, dichos datos deben ser enviados en forma encriptada, siempre y cuando el receptor tenga los recursos necesarios y acepte el intercambio de datos cifrados. El Área de Ingeniería brindará asesoría y acompañamiento en el proceso de Cifrado.

- ✓ Eliminación Segura de la Información en Medios Informáticos: Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por SERVERS & SOFTWARE S.A.S antes de su entrega se les realizara un proceso de borrado seguro en la información.

- ✓ Eliminación segura de la información en medios físicos: Cualquier documento físico que haya sido considerado y clasificado de carácter confidencial y que necesite ser destruido, debe realizarse en la respectiva maquina destruye papel o cualquier otro método seguro de destrucción.

El área de Ingeniería, debe definir un procedimiento de gestión de claves, donde incluirán los métodos para la generación, longitud, eliminación y recuperación de claves en caso de pérdida, divulgación o daño.

7.2.TRANSFERENCIA DE LA INFORMACIÓN

Toda la información que se reciba o envié a través de impresoras u otros medios de litografía y transmisión de datos, debe ser monitoreada por el funcionario que los esté utilizando y debe permanecer siempre sin ningún tipo de documentos o información clasificada como de uso interno o reservada.

El área de Ingeniería debe realizar capacitaciones y/o difundir los lineamientos de la compañía para evitar que se traten temas de la compañía en sitios públicos o escenarios no autorizados formalmente para la divulgación de información.

Salvo casos de estricta necesidad y bajo previa autorización y/o recomendación. no se suscribirán o diligenciarán formularios electrónicos para uso personal o para medios de investigación a través de Internet, así mismo se debe evitar el diligenciamiento de los datos de ubicación física, teléfonos móviles, teléfonos fijos, estructura organizacional, divulgación de cargos o información sensible de la compañía, cuando el personal se suscriba o diligencie formularios electrónicos para uso personal o para medios de investigación a través de Internet.

La recepción de correspondencia únicamente podrá ser revisada y visualizada por el destinatario de los documentos

7.3.PROTECCIÓN CONTRA ROBO

- ✓ Los sistemas, equipos de red y dispositivos USB deben asegurarse físicamente cuando se encuentren en oficinas o lugares abiertos.

- ✓ Tanto los equipos de red, servidores y otros sistemas multiusuario deben estar ubicados en lugares con control de acceso.

- ✓ Los computadores portátiles deben estar asegurados por un cable, ubicados en gabinetes cerrados o asegurados cuando se encuentren en lugares no vigilados.

- ✓ En lo posible, utilice un software de cifrado para resguardar con mayor seguridad los datos almacenados en su portátil, para ello, es recomendable elegir una frase larga, contraseña de cifrado fuerte y mantenerlos seguros. El Área de Ingeniería le brindará la información y asesoría necesaria para llevar a cabo esta actividad. De

esta manera, si su portátil se pierde o es robado, la configuración de cifrado proporciona una protección muy fuerte contra el acceso no autorizado a los datos.

- ✓ El empleado que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad de la información deberá reportarlo al Jefe Inmediato y al Líder de Ingeniería lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad de la información.

- ✓ Cuando exista la sospecha o el conocimiento que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización debida, el empleado deberá notificar a su Jefe Inmediato y al Líder de Ingeniería.

- ✓ Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de SERVERS & SOFTWARE S.A.S debe ser reportado a la Dirección Administrativa y Financiera y al Líder de Ingeniería-mesa de ayuda.

7.4. POLÍTICA DE ESCRITORIO LIMPIO

La política de escritorios y pantallas despejadas es extensiva para todos los funcionarios, contratistas de SERVSOFT y apoya en la seguridad de la información sensible o crítica de la compañía.

Los objetivos específicos de este capítulo relacionado con el uso de escritorios y pantallas despejadas son:

- Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.
- Crear conciencia sobre los riegos asociados al manejo de información tanto física como digital y la manera de reducirlos aplicando los lineamientos aquí determinados.
- Especificar las recomendaciones y pautas necesarias para mantener las pantallas y escritorios organizados y controlando el reposo de información clasificada o reservada a la vista.
- Dictar las pautas para mantener organizado y resguardado los documentos digitales y correos electrónicos en los computadores puestos a disposición de todos los usuarios de los sistemas de información y estructura tecnológica del SERVSOFT

Este lineamiento se define en el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico como tecnológico entendiéndose para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada funcionario, contratista o practicante de la compañía y pantalla, el área de trabajo virtual sobre el sistema operativo de su

computador, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Institucionales.

El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los funcionarios, contratistas y practicantes que tengan acceso a la información del SERVSOFT SA, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:

ESCRITORIOS

- Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.
- En la medida de lo posible los documentos con información clasificada o reservada debe quedar bajo llave o custodia en horas no laborables.
- Se debe evitar el retiro de documentos clasificados o reservados de la institución y en el caso de ser necesario se debe propender por su protección fuera del Instituto y su pronta devolución al mismo.
- Se debe restringir el fotocopiado de documentos fuera del horario normal de trabajo y fuera de las instalaciones de la compañía. De ser necesario se debe autorizar el retiro de dichos documentos y garantizar su protección y confidencialidad fuera.
- Al imprimir o fotocopiar documentos con información clasificada o reservada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.
- No se debe reutilizar papel que contenga información clasificada o reservada.

PANTALLAS

- Los computadores o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y los mismos deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso a los mismos. Es responsabilidad del usuario, asegurar que el equipo tenga la protección adecuada
- Las áreas de trabajo virtuales "pantallas" del computador deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información y a carpetas y unidades de red necesarios para la ejecución de las actividades.
- Los documentos digitales deben ser organizados en carpetas y evitar dejarlos a la vista en las pantallas de los computadores.
- Los funcionarios y contratistas al retirarse de la oficina deben apagar los computadores asignados. Queda fuera de esta indicación los servidores y

estaciones de trabajo utilizados para acceso remoto. Las sesiones activas se deben terminar cuando el usuario finalice las actividades programadas.

- El área de ingeniería determinará una configuración automática en todos los equipos de cómputo, propiedad o contratados para que se active el bloqueo de sección de pantalla del computador, bloqueando el acceso al computador al presentarse una inactividad de 5 minutos. Estos pueden ser nuevamente utilizados por los usuarios al volver a realizar la autenticación por medio de los usuarios y contraseñas asignados.
- El fondo de pantalla de cada computador es único para todas las estaciones de trabajo y para todos los usuarios y puede ser cambiado únicamente por el área de ingeniería.

MONITOREO

- El área de ingeniería sin previo aviso, realizan brigadas de monitoreo para verificar el estado de los computadores, monitores y escritorios virtuales y generar el respectivo informe de lo encontrado.

8. CONTROLES DE SEGURIDAD LÓGICA Y FÍSICA

8.1. IDENTIFICACIÓN Y AUTENTICACIÓN DEL USUARIO

Cada empleado es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y claves necesarios para acceder a la información y a la infraestructura tecnológica de SERVERS & SOFTWARE por lo cual deberá mantenerlo de forma confidencial.

8.2. USUARIO Y CLAVE

- ✓ SERVERS & SOFTWARE S.A.S requiere que todos los empleados que tengan acceso a sus recursos tecnológicos dispongan de un Usuario y una Clave de carácter privado, personal e intransferible.

Es responsabilidad de Recursos Humano informar al área de Ingeniería, sobre los nuevos administrativos, contratistas y/o que ingresan a la compañía, con el fin de poder asignar, los respectivos permisos para el acceso a los recursos tecnológicos de la compañía.

- ✓ La asignación del Usuario y Clave debe estar acorde a las funciones, responsabilidades y actividades del usuario.

- ✓ El acceso a la infraestructura tecnológica de SERVERS & SOFTWARE S.A.S para personal externo debe ser autorizado por la Gerencia, la cual deberá notificarlo al Líder de Ingeniería, quien lo habilitará.

- ✓ Todos los empleados tienen la obligación de proteger sus datos de autenticación.

- ✓ Los empleados no deben proporcionar información a personal externo de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de SERVERS & SOFTWARE S.A.S, a menos que se tenga la autorización de la Gerencia.

- ✓ Cada empleado que acceda a la infraestructura tecnológica de SERVERS & SOFTWARE S.A.S debe contar con un Identificador de Usuario (UserID) único y personalizado, por lo cual no está permitido el uso de un mismo UserID por varios empleados.

- ✓ Cualquier cambio en los roles y responsabilidades de los empleados que modifique sus privilegios de acceso a la infraestructura tecnológica de SERVERS & SOFTWARE S.A.S deberá ser notificado al Líder de Ingeniería con el visto bueno de su Jefe Inmediato.

- ✓ Cuando un empleado olvide, bloquee o extravíe su Clave deberá informarlo al Área de Ingeniería para que se le proporcione una nueva Clave y una vez que la reciba deberá cambiarla en el momento en que acceda nuevamente a la infraestructura tecnológica.

- ✓ Está prohibido que las Claves se encuentren de forma legible en cualquier medio impreso y dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.

- ✓ La Clave de servidores tendrá una vigencia de 30 días.

- ✓ Los empleados no deben almacenar las claves en ningún programa o sistema que proporcione esta facilidad.

- ✓ Las claves no deben ser guardadas en archivos que puedan ser leídos, computadores sin control de acceso o en lugares donde personal no autorizado tenga acceso.

8.3. ELECCIÓN DE UNA CLAVE

Los empleados deben elegir una Clave que sea difícil de adivinar y que no contenga información relativa a la vida personal. Por ejemplo, no debe contener el número de la cédula, la fecha de nacimiento, número de teléfono, nombre de familiares (esposa, esposo, hijo), nombre de la mascota, etc.

Algunos consejos para la creación de claves.

- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos.
- Combinar varias palabras. Combinar palabras con signos de puntuación o números, caracteres mayúsculas y minúsculas.
- Transformar una palabra común utilizando un método específico y personal.
- Crear acrónimos.
- Deliberadamente utilizar mal una palabra o escribirla mal ortográficamente.
- No deben ser idénticos o similares a claves que hayan sido usados previamente.
- No utilice la misma clave para los diferentes sistemas o puntos de acceso al que esté autorizado.
- Cuando la información requiera ser compartida los empleados deben hacerlo utilizando e-mails, bases de datos, y directorios públicos ubicados en la red con controles de acceso y otros medios de intercambio de información.
- Las claves en ningún momento deben ser compartidas o divulgadas.
- Si se advierte que un empleado está utilizando los datos de autenticación (Usuario y Clave) de otro empleado, es su responsabilidad avisar de este evento a su Jefe Inmediato y al Líder de Ingeniería.

SOFTWARE MALICIOSO

8.4. SOFTWARE DE DETECCIÓN DE VIRUS

- ✓ Los empleados no deberán cancelar los procesos automáticos de actualización de las definiciones de virus.

- ✓ Todos los sistemas deben ser analizados por un antivirus.

- ✓ Un scan debe ser ejecutado antes de abrir un archivo nuevo y después de ejecutar un software nuevo. El antivirus instalado en el computador deberá garantizar este proceso de manera automática.

- ✓ Para prevenir infecciones por virus informático los empleados de SERVERS & SOFTWARE S.A.S no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el Área de Ingeniería.

- ✓ Los empleados de SERVERS & SOFTWARE S.A.S deben verificar que la información y los medios de almacenamiento, considerando que al menos unidades USB, CD's, cintas y cartuchos, estén libres de cualquier tipo de software malicioso o virus, para lo cual deben ejecutar el software antivirus autorizado por el Área de Ingeniería.

- ✓ Todos los archivos de computadora que sean proporcionados por personal externo o interno en relación con programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, deben ser verificados por el empleado de que estén libres de virus utilizando el antivirus autorizado antes de ejecutarse.

- ✓ Ningún empleado de SERVERS & SOFTWARE S.A.S debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir códigos de computadora diseñados para auto replicarse, dañar, o, en otros casos, impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas de SERVERS & SOFTWARE S.A.S. El incumplimiento de este estándar será considerado una falta grave.

- ✓ Ningún empleado o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Líder de Ingeniería.

- ✓ Cualquier empleado que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Área de Ingeniería para la detección y erradicación del virus.

- ✓ Cada empleado que tenga bajo su resguardo algún equipo de computador portátil asignado por SERVERS & SOFTWARE S.A.S y que dicho activo no esté conectado permanentemente a la red de la organización, será responsable de solicitar periódicamente al Área de ingenieria de las definiciones de virus.

- ✓ Los empleados no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por SERVERS & SOFTWARE S.A.S en: Antivirus, Outlook, Office, Navegadores u otros programas.

- ✓ Todos los medios removibles y otros medios de almacenamiento electrónico sobre un computador infectado no deberán ser utilizados sobre otro computador hasta que el virus haya sido removido de manera exitosa.

- ✓ El computador infectado deberá ser retirado de la operación para su revisión oportuna y efectiva.

- ✓ Debido a que algunos virus son extremadamente complejos ningún empleado de SERVERS & SOFTWARE S.A.S debe intentar erradicarlos de las computadoras.

- ✓ El Área de Ingeniería será el encargado o responsable de llevar a cabo las acciones para la remoción del virus y garantizar la pérdida mínima de información, minimizar los daños y el tiempo fuera de servicio del computador infectado.

9. SEGURIDAD DE LA RED

9.1. CONEXIONES A LA RED INTERNA

- ✓ Todos los computadores que contengan información sensible o crítica deben estar conectados a la red de la organización, y disponer de controles de acceso aprobados por el Área de Ingeniería.

- ✓ Todos los sistemas de procesamiento de información deben estar configurados de forma tal que durante un tiempo de inactividad sea bloqueada la pantalla y el acceso al sistema. Una vez el empleado indique los datos de autenticación podrá ingresar de nuevo al sistema.

- ✓ Los sistemas multiusuario deben usar mecanismos de cierre de sesión que automáticamente bloqueen el usuario durante un tiempo de inactividad.

- ✓ Los empleados no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP USMB1ya que tienen protocolos de compatibilidad y pueden afectar los protocolos y servicios), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de SERVERS & SOFTWARE S.A.S sin la autorización del Líder de Ingeniería.

- ✓ Será considerado como un ataque a la seguridad de la información y una falta grave contra SERVERS & SOFTWARE S.A.S cualquier actividad no autorizada por

el Área de Ingeniería en la cual los empleados realicen la exploración de los recursos informáticos en la red, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

9.2.**CONEXIONES A LA RED EXTERNA**

- ✓ Las conexiones a los sistemas de información de SERVERS & SOFTWARE S.A.S deben estar protegidas y aseguradas por un sistema de control de acceso dinámico de forma tal que se garantice la unicidad de claves para cada acceso.

- ✓ Los empleados no deben establecer conexiones a redes externas sin la aprobación del Líder de Ingeniería

- ✓ La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el Líder de Ingeniería.

- ✓ Cambios en la red.

Todos los cambios en la configuración de la red deben tener un registro que formalice dicho cambio y deben ser aprobados por el Líder de Ingeniería.

Todos los cambios a la red interna deben ser realizados por el Área de Ingeniería. Este procedimiento reduce el riesgo de divulgación no autorizada y que los cambios realizados sean hechos de manera pertinente y con el conocimiento y aprobación del Líder de Ingeniería. Este proceso aplica no sólo al personal de SERVERS & SOFTWARE S.A.S sino también a los proveedores de servicios o personal externo.

- ✓ Trabajo Remoto, Teletrabajo o trabajo desde casa

Sólo los empleados autorizados por la Gerencia tendrán acceso remoto única y exclusivamente a través de una VPN (Red Privada Virtual) a los sistemas de SERVERS & SOFTWARE S.A.S, no está permitido el acceso remoto utilizando conexiones diferentes a una VPN.

El Área de Ingeniería llevará un registro de los empleados autorizados por la Gerencia para acceder de manera remota a los sistemas de SERVERS & SOFTWARE S.A.S y asistirá en la configuración de la conexión VPN a aquellos usuarios que hayan sido autorizados. De estos accesos deberán llevarse un Logg.

La continuidad de estas autorizaciones estará sujeta al cumplimiento de las Políticas de Seguridad de la información y la revocatoria de la autorización estará a cargo de la Gerencia General.

- ✓ Servicios de Outsourcing – Subcontratación.

El Outsourcing, definido como la gestión o ejecución temporal o permanente de una función empresarial por un proveedor externo de servicios, debe ser controlado dado los riesgos potenciales que implica el acceso (Virtual o Físico) de éste a las instalaciones fisicas, a la información, a los activos. Riesgos como por ejemplo el acceso inadecuado, divulgación de información, impericia del subcontratista, pérdida de la propiedad intelectual, falta de apropiamiento (Sentido de Pertenencia), etc.

Se considera como proveedores de Outsourcing quienes:

- Ofrecen soporte de Hardware y software y al personal de mantenimiento
- Consultores externos y contratistas
- Empresas TI de externalización de procesos empresariales
- Personal temporal

Se deben registrar o documentar los Controles de acceso para restringir la divulgación no autorizada, modificación o destrucción de la información, incluyendo controles de acceso físico y lógico, los procedimientos para conceder, revisar, actualizar y revocar el acceso a los sistemas, datos e instalaciones. Estos controles deben ser definidos entre la Jefatura Administrativa y Financiera y el Área de Ingeniería con la aprobación de la Gerencia.

10. POLÍTICAS GENERALES DE LA GERENCIA

- ✓ Evaluación y tratamiento del riesgo: La evaluación de riesgos debe identificar, cuantificar y priorizar los riesgos frente a los criterios de aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deben guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos.

  El alcance de la evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil.

Se debe realizar una evaluación de riesgos a los recursos informáticos de SERVERS & SOFTWARE S.A.S S.A. por lo menos una vez al año utilizando el procedimiento Interno: "Análisis de riesgos"

- ✓ Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos. No se otorgarán privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por la Gerencia.

- ✓ Los sistemas de comunicación deben tener controles de acceso físico apropiados.

  Todos los equipos de comunicaciones, otros equipos que contengan información sensible y el software licenciado de propiedad de la compañía deben ubicarse en centros de cómputo con puertas cerradas y controles de acceso físico apropiados.

- ✓ Entrenamiento compartido para labores técnicas críticas. Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración de los sistemas de información críticos de SERVERS & SOFTWARE S.A.S.

- ✓ Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias. Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se debe crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor. La contingencia de sistemas que se acuerdan con terceros deberá disponer de una infraestructura y de un modelo de soporte acorde a las necesidades de SERVERS & SOFTWARE S.A.S

- ✓ Personal competente en el Área de Sistemas para dar pronta solución a problemas.

  Con el fin de garantizar la continuidad de los sistemas de información, SERVERS & SOFTWARE S.A.S. deben contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

- ✓ Chequeo de virus en archivos recibidos en correo electrónico. SERVERS & SOFTWARE S.A.S debe procurar y disponer de los medios para que todos los

archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores de los usuarios.

- ✓ Contacto con grupos especializados en seguridad de la información. El personal involucrado con la seguridad de la información deberá tener contacto con grupos especializados o foros relacionados con la seguridad de la información. Esto con el objetivo de conocer las nuevas medidas en cuanto a seguridad de la información se van presentando.

  En casos de emergencia manifiesta, que estamos afectando directamente la normal prestación de los servicios de la compañía en cualquiera de sus unidades, se podrán realizar cambios en la configuración de recursos y servicios de infraestructura tecnológica

11. CUMPLIMIENTO

El Área de Ingeniería y el área de sistemas de gestión realizarán periódicamente Auditorías de Seguridad para garantizar el cumplimiento de las políticas aplicables, los procedimientos y la legislación.

El Comité de Seguridad de la información tiene como una de sus funciones proponer y revisar el cumplimiento de las normas y políticas de seguridad que garanticen acciones preventivas y correctivas para la salvaguarda de los equipos e instalaciones de cómputo, así como de los bancos de datos de información automatizada en general.

Está prohibido por las leyes de derechos de autor y por SERVERS & SOFTWARE S.A.S realizar copias no autorizadas de software, ya sea adquirido o desarrollado por SERVERS & SOFTWARE S.A.S

Los sistemas desarrollados por el personal interno o externo que controle el Área de Ingeniería son propiedad intelectual de SERVERS & SOFTWARE S.A.S.

11.1. CUMPLIMIENTO DE LAS POLÍTICAS Y PROCEDIMIENTOS

- ✓ Todos los empleados deben cumplir con las Políticas de Seguridad de la información y sus documentos relacionados. Los empleados que por negligencia violen estas normas serán objeto de sanciones disciplinarias o despido.

- ✓ El Área de Ingeniería y el área de sistemas de gestión, realizarán acciones de verificación del cumplimiento de Políticas de acuerdo con lo establecido en su Plan Anual de Trabajo.

- ✓ El Área de Ingeniería y sistemas de Gestión podrán implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, con el fin de revisar la actividad de los procesos que ejecuta y la estructura de los archivos que se procesan.

- ✓ El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad de la información.

- ✓ Los empleados que sean propietarios de la información deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y cualquier otro requerimiento de seguridad.

11.2. CUMPLIMIENTO DE LA LEGISLACIÓN Y NORMATIVIDAD

Todas las Políticas de Seguridad de la información deben cumplir con la legislación aplicable, como las leyes de protección de datos, acceso a la información, protección de información personal y documentos electrónicos.

11.3. MEDIDAS DISCIPLINARIAS

Las violaciones sospechosas de la Política de Seguridad de la información (penetración del sistema, infección de virus) que podrían comprometer la integridad de los sistemas de información deben ser reportadas oportunamente al Jefe Inmediato y al Área de Ingeniería.

La violación comprobada o el incumplimiento de la Política de Seguridad de la información suponen graves consecuencias para los infractores y medidas disciplinarias que varían de acuerdo a la severidad de la violación y puede ocasionar el despido del infractor.

SERVERS & SOFTWARE S.A.S reconoce abiertamente la importancia de la seguridad de la información, así como la necesidad de su protección para constituir un activo estratégico de la organización y todas las partes interesadas, el no uso adecuado de los activos de información puede poner en peligro la continuidad del negocio o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

SERVERS & SOFTWARE S.A.S podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal, por solicitud de autoridad judicial o administrativa salvo las excepciones indicadas en este documento y las disposiciones legales de protección de datos personales.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

12. NOTAS

- ✓ Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.

- ✓ El documento que contiene la política de seguridad deber ser difundido a todo el personal involucrado en la definición de estas políticas.

CARLOS HUMBERTO GUZMAN GOMEZ
Gerente General
Bogotá D.C., 19 mayo de 2023

CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCION DEL CAMBIO
07/10/2020	1	Elaboración y aprobación del documento
08/04-2021	2	Revisión y actualización de la política de seguridad de la información por el Coordinador del área de ingeniería-mesa de ayuda, sin observaciones.
03/01/2023	3	Revisión general del documento por líder de ingeniería y líder de proyectos, se actualiza alcance Revisión y firma por la Gerencia.
19/05/2023	4	Cambio de terminología seguridad informática por seguridad de la información