POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA VIASERVIN LTDA.

Con el objetivo de respaldar el Sistema de Gestión de Seguridad de la Información en VIASERVIN LTDA, se ha decidido establecer, poner en práctica, operar y mejorar de manera continua el Sistema de Gestión de Seguridad de la Información con la participación de todos los involucrados. Este sistema estará fundamentado en las siguientes políticas generales:

- Todos los empleados de la empresa están obligados a leer y cumplir con el Manual de Seguridad de la Información, asumiendo la responsabilidad sobre la seguridad de la información que sea compartida, publicada y aceptada por cada uno de los colaboradores, contratistas y terceros.
- Se tomarán las medidas necesarias para proteger la información frente a vulnerabilidades que puedan originarse por parte de los empleados, contratistas y terceros, y el proceso de Seguridad de la Información será el único autorizado para verificar y validar cualquier incidente de seguridad.
- Se implementarán controles de acceso para proteger la información, los sistemas y los recursos de red, con el objetivo de salvaguardar nuestras instalaciones e infraestructura tecnológica que soportan los procesos de la empresa.
- Se llevará a cabo un proceso de mejora continua en la seguridad y privacidad de la información, gestionando adecuadamente los procesos para identificar posibles debilidades y cualquier incidente relacionado con la seguridad.
- VIASERVIN LTDA. se compromete a cumplir con todas las obligaciones legales, regulatorias y contractuales que correspondan.

Cualquier incumplimiento de la política de Seguridad y Privacidad de la Información acarreará las consecuencias legales pertinentes, conforme al reglamento interno y a lo estipulado por las normas del gobierno nacional y local relacionadas con la seguridad y privacidad de la información.

1.1. LINEAMIENTO DE ACCESO A LA INFORMACIÓN

Todos los colaboradores, que laboran para la empresa VIASERVIN LTDA deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a VIASERVIN LTDA, la Gerencia, jefes de Oficina y/o responsables de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Todas las prerrogativas para el uso de los sistemas de información de la Organización deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Organización

Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Organización, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Organización.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Organización, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

1.2. LINEAMIENTO DE ADMINISTRACIÓN DE CAMBIOS

Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración de este, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá las facultades de aceptar o rechazar la solicitud.

En ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.
Para la administración de cambios se efectuará el procedimiento correspondiente definido por VIASERVIN LTDA, de acuerdo con el tipo de cambio solicitado.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

1.3. LINEAMIENTO SEGURIDAD DE LA INFORMACIÓN

Los colaboradores, proveedores, contratistas, etc. de VIASERVIN LTDA son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Organización, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los colaboradores, proveedores, contratistas, no deben suministrar cualquier información de la Organización a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los Recursos Informáticos tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Los colaboradores, proveedores, contratistas deben firmar, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Organización, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario, contratistas, de VIASERVIN LTDA deben comprometerse a no utilizar, comercializar o divulgar los productos o a información generada o conocida durante la gestión en la Organización, directamente o través de terceros, así mismo, los colaboradores que detecten el mal uso de la información está en la obligación de reportar el hecho a su jefe inmediato.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a colaboradores y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

1.4. LINEAMIENTO DE SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS

El internet, sistema de correo electrónico, software de chateo y utilidades asociadas de la Organización debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los practicantes, proveedores y contratistas.

La Organización se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, el funcionario o contratista autorizará a la Organización para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros. Los colaboradores, practicantes, proveedores, contratistas etc. no deben utilizar versiones escaneadas de Firmas hechas a mano para dar la impresión de un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmado por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Organización. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

Los colaboradores, contratistas que hayan recibido aprobación para tener acceso a

Internet a través de las facilidades de la Organización, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

En cualquier momento que un trabajador publique un mensaje en un grupo de discusión de Internet, en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición de la Organización.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de sistemas, no utilizar el computador y desconectarlo de la red.

El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "Clausula de Responsabilidad".

El Jede de Sistemas debe proveer material para recordar regularmente a los empleados, temporales, practicantes, proveedores y contratistas acerca de sus obligaciones con respecto a la seguridad de los recursos informáticos.

1.5. LINEAMIENTO DE SEGURIDAD EN RECURSOS INFORMÁTICOS

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos. Establece parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de estas, entre otras. La contraseña debe incluir mínimo 8 caracteres entre ellos minúsculas, mayúsculas, números y símbolos. Esta debe cambiarse al momento del pc solicitarlo es cual esta configurado para 42 dias.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el Administrador de usuarios.

Plan de auditoria: Hace referencia a las pistas o registros de los sucesos relativos a la operación.

Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de estas en la mayoría de los sistemas operacionales, bases de datos,

aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

El control de acceso a todos los sistemas de computación de la Organización debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los colaboradores , contratistas, etc. De VIASERVIN LTDA son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

El nivel de administrador o superusuario de los sistemas críticos debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de ciframiento para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los subdirectores, jefes de oficina, en conjunto con el jefe de seguridad informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

1.6. LINEAMIENTO DE SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Organización, deberán ser consideradas y tratadas como información confidencial.

La red de amplia cobertura geográfica a nivel nacional e internacional debe estar dividida en forma lógica por diferentes segmentos de red, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Todo intercambio electrónico de información o interacción entre sistemas de información con Organizaciones externas deberá estar soportado y autorizado por Gerencia y Direccion de electrónica.

Los computadores de OEG se conectarán de manera directa con computadores de Organizaciones externas, conexiones seguras, previa autorización del área de sistemas y/o la oficina de informática.

Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Organización e Internet deberá estar cifrada

1.7. LINEAMIENTO DE SEGURIDAD PARA USUARIOS TERCEROS

Los dueños de los Recursos Informáticos que no sean propiedad de la Organización y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

Cuando se requiera utilizar recursos informáticos u otros elementos de propiedad de VIASERVIN LTDA para el funcionamiento de recursos que no sean propios de la Organización y que deban ubicarse en sus instalaciones, los recursos serán administrados por el área técnica de VIASERVIN LTDA.

Los usuarios terceros tendrán acceso a los Recursos Informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el jefe inmediato o coordinador.

La empresa VIASERVIN LTDA se reserva el derecho de permitir a los usuarios, contratistas, terceros, etc., la utilización de sistemas de almacenamientos de información como USB, CD, DVD, DISCOS EXTERNOS o cualquier otro sistema que pudiera poner en riesgo la integridad de la información o su plataforma de red. Deberá existir una autorización de la Administración o Gerencia para tal fin.

La conexión entre sistemas internos de la Organización y otros de terceros debe ser aprobada y certificada por el Área de Sistemas con el fin de no comprometer la seguridad de la información interna de la Organización.

Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad informática vigentes en la Organización.

Como requisito para interconectar las redes de la Organización con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la Organización. La Organización se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La Organización se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la Organización.

1.8. LINEAMIENTO DE SOFTWARE UTILIZADO

Todo software que utilice la empresa VIASERVIN LTDA será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Organización o reglamentos internos.

Todo el software de manejo de datos que utilice la empresa VIASERVIN LTDA dentro de su infraestructura informática, deberá estar previamente autorizado por el área de dirección de electrónica y gerencia.

Debe existir una cultura informática al interior de la Organización que garantice el conocimiento por parte de los colaboradores, contratistas, etc., de las implicaciones que tiene el instalar software ilegal o no autorizado en los computadores de la empresa VIASERVIN LTDA.

1.9. LINEAMIENTO DE ACTUALIZACIÓN DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la Organización (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal de sistemas.

Los equipos de microcomputadores (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada.

1.10. LINEAMIENTO DE ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática de Viaservin Ltda deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

La Organización definirá la custodia de los respaldos de la información.

El almacenamiento de la información deberá realizarse interna y/o externamente a la Organización, esto de acuerdo con la importancia de la información para la operación.

El área dueña de la información en conjunto con la oficina de sistemas definirá la estrategia a seguir para el respaldo de la información.

Los colaboradores son responsables de los respaldos de su información en los microcomputadores, siguiendo las indicaciones técnicas dictadas por la oficina de sistemas. La oficina de informática será la autorizada para realizar el seguimiento y control de esta política.

1.11. LINEAMIENTO DE CONTINGENCIA

La administración de la Organización debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

1.12. LINEAMIENTO DE AUDITORIA

Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

Todos los archivos de auditorias de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

Todos los archivos de auditorías deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

Todos los computadores de la Organización deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

1.13. LINEAMIENTO DE SEGURIDAD FÍSICA

La Organización deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la Organización considere críticas.

Los visitantes de las oficinas de la Organización deben ser escoltados durante todo el tiempo por un empleado autorizado, asesor o contratista, etc,. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada.

Siempre que un trabajador se dé cuenta que un visitante no es escoltado se encuentra dentro de áreas restringidas de la Organización, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

Los centros de cómputo o áreas que la Organización considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

Toda persona que se encuentre dentro de la Organización deberá portar su identificación en lugar visible.

En los centros de cómputo o áreas que la Organización considere criticas deberán existir elementos de control de incendio, inundación y alarmas.

Los centros de cómputo o áreas que la Organización considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la Organización a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la oficina de sistemas.

Todos los visitantes deben mostrar identificación con fotografía y firmar antes de obtener el acceso a las áreas restringidas controladas por la Organización.

Los equipos de microcomputadores (PC, portátiles, Servidores, equipos de comunicaciones, etc.) no deben moverse o reubicarse sin la aprobación previa.

Los colaboradores se comprometen a NO utilizar a la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como cargadores de celulares, grabadoras, electrodomésticos y en general cualquier equipos que generen caídas de la energía.

Los particulares en general, entre ellos, los familiares de los colaboradores, no están autorizados para utilizar los recursos informáticos de la Organización.

1.14. LINEAMIENTO DE ESCRITORIOS LIMPIOS

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, DVD,s disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

1.15. LINEAMIENTO DE ADMINISTRACIÓN DE LA SEGURIDAD

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada año, Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al Asesor de Sistemas.