

1. OBJETIVO

Proteger los recursos de información de Servicios Integrales y los sitios donde cuente con infraestructura tecnológica para el cumplimiento de las obligaciones contractuales y se encuentre en operación el Software SIOT y la tecnología utilizada para su procesamiento frente a amenazas internas o externas, deliberadas o accidentales, con el fin de garantizar la confidencialidad, integridad, disponibilidad, no repudio y legalidad de la información.

2. ALCANCE

Aplica para todas las estaciones de trabajo de Servicios Integrales y/o Centros de Producción que esta administre.

3. DEFINICIONES

- **Privilegios:** Permisos de acceso a aplicativos y/o redes.
- **VPN:** Red Privada Virtual
- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **No repudio:** Una autenticación que con un alto aseguramiento pueda ser reafirmado como genuino
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

4. POLÍTICAS

4.1. Política Corporativa de Seguridad de la Información

En Servicios Integrales y en cada uno sitios donde cuente con infraestructura tecnológica para el cumplimiento de las obligaciones contractuales y se encuentre en operación el Software SIOT, la información es un activo fundamental para la prestación de sus servicios, razón por la cual existe un compromiso expreso de protección de sus

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio y la consolidación de una cultura de seguridad.

Para conseguir su objetivo, Servicios Integrales implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información.

Esta política será revisada anualmente como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición especial, buscando asegurar su vigencia e implementación.

Se tomarán las acciones disciplinarias por el incumplimiento de las siguientes políticas por parte de los empleados descritas en el documento externo **Reglamento Interno de Trabajo**, en el capítulo XVIII de Sanciones disciplinarias.

4.2. Políticas generales de seguridad de la información

- El Gerente de Tecnología de la Información, será la responsable de garantizar del mantenimiento, revisión y mejora de los controles implementados en la Seguridad de la Información de la empresa.
- Los activos de información serán identificados para establecer los mecanismos de protección necesarios.
- Servicios Integrales implementa controles en busca de garantizar la confidencialidad, integridad y disponibilidad de la información.
- Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual tienen acceso y pueden procesar buscando evitar su pérdida, alteración, destrucción o uso indebido.
- Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente con licenciamiento o de libre distribución.
- Es responsabilidad de todos los funcionarios y contratistas de Servicios Integrales reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Servicios Integrales para realizar las pruebas del software SIOT, hacer uso de bases de datos de prueba las cuales no contiene información sensible o real que comprometa la confidencialidad de la información. De igual forma se cuenta con los controles de acceso y restricciones de usuario a esta información.

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

- La información de bases de datos de prueba, no será utilizada para ningún otra actividad diferente a la realización de pruebas de funcionamiento del Software SIOT.
- Servicios Integrales garantiza que la información contenida en las estaciones de trabajo del personal y contratistas está protegida contra la fuga de información mediante controles de acceso y permisos de usuario establecidos.

Adicionalmente, a continuación, se definen políticas específicas y procedimientos que soportan la política corporativa.

4.3. Acuerdos de confidencialidad. [ISO/IEC 27001:2005 A.6.1.5]

Todos los empleados de Servicios Integrales y/o terceros deben aceptar los acuerdos de confidencialidad definidos, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad. Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Para el caso de sitios donde cuente con infraestructura tecnológica para el cumplimiento de las obligaciones contractuales y se encuentre en operación el Software SIOT, pero de administración del cliente, se les darán las políticas de forma informativa, pero será su decisión el adoptarlas.

4.4. Acceso a Internet [ISO/IEC 27001:2005 A.11.4]

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

- No está permitido:
 - El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
 - El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares,

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio. Solo se autorizará el uso de Skype a las personas que dentro de sus funciones tengan la labor de brindar soporte o realizar acompañamiento a procesos por fuera de la oficina principal. Esta autorización será concedida en el acta de entrega del equipo de cómputo.

- El intercambio no autorizado de información de propiedad de Servicios Integrales, de sus clientes y/o de sus empleados y/o información estratégica, con terceros.
- Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.
- El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la empresa o los Centros de Producción que esta administre.

4.5. Correo electrónico [ISO/IEC 27001:2005 A.10.8.4]

Los funcionarios y terceros autorizados a quienes Servicios Integrales les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

- La cuenta de correo electrónico debe ser usada exclusivamente para el desempeño de las funciones asignadas dentro de Servicios Integrales o el Centro de Producción.
- Los mensajes y la información contenida en los buzones de correo son propiedad de Servicios Integrales o del Centro de Producción y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- El tamaño de los buzones de correo es determinado por la Gerencia Operaciones y Tecnología de la Información, de acuerdo con las necesidades de cada usuario, o de acuerdo a la disponibilidad otorgada por el licenciamiento del motor de correo electrónico.
- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que Servicios Integrales proporciona. De igual manera, las cuentas de correo genéricas, serán asignadas por la Gerencia de Tecnologías de la Información y asignadas en el formato establecido.

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

- El envío y recepción de archivos adjuntos está permitido a excepción de archivos maliciosos, scripts o modificadores de registros. Al descargar estos adjuntos deben ser analizados por el software de antivirus vigente.

4.6. Clasificación y Uso de la Información. [ISO/IEC 27001:2005 A.7.2]

Los jefes de área responsables de la información contenida en los departamentos a su cargo, deben delimitar las responsabilidades de sus subordinados y determinar quién está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Ningún tercero en proyectos de software y/o trabajos específicos, deberá poseer para usos no propios de su responsabilidad ningún material o información confidencial de la compañía tanto ahora como en el futuro.

Se definen las siguientes categorías para clasificar la información en la compañía:

- **Restringida:** Información extremadamente sensible al interior de la compañía y que puede ser conocida únicamente por cierto número de funcionarios.
- **Reservada:** Información sensible al interior de la compañía y es para uso exclusivo de un grupo específico de colaboradores.
- **Interna:** Información disponible solo para los funcionarios de la compañía.
- **Publica:** Información no sensible que puede ser conocida tanto por el personal de la compañía como por terceros sin poner en riesgo la imagen institucional.

El software, documentación digital y demás tipos de información física expresa de la empresa, no deben ser compartida, puesta en venta ni transferida a ningún ente sin previa autorización expresa por la Gerencia general.

No se debe otorgar nombre de usuario, contraseñas ni privilegios de ningún nivel para utilizar infraestructura tecnológica como equipos de cómputo, red LAN, servicios informáticos a personas que no pertenecen a Servicios Integrales sin previa autorización del área de informática y la Gerencia Tecnología de la Información

Información Restringida: Los empleados de Servicios Integrales en todo momento se abstendrán de:

- Realizar o aconsejar cualquier operación en provecho propio o de terceros utilizando la información privilegiada.

REVISO: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

Se considera información confidencial y/o privilegiada la siguiente:

- Estados financieros y proyecciones económicas.
 - Listas de clientes y proveedores.
 - Elementos de propiedad intelectual e industrial (Código Fuente de Aplicaciones propias).
 - Formatos y/o archivos digitales de seguimiento y/o control de las actividades desarrolladas en cada una de las áreas en el día a día.
 - Datos personales de los trabajadores
- Suministrar a un tercero, información confidencial, sin autorización. Además, los empleados de la Compañía mantendrán la debida reserva y protegerán en todo momento los documentos de trabajo y la información confidencial que tengan a su cuidado, y por lo tanto:
 - No comentarán temas de la compañía con personal ajeno a ésta, incluyendo amigos o parientes.
 - Proyectos de la empresa, especialmente aquellos que incluyan información confidencial, no se tratarán en lugares donde haya terceros y guardarán discreción extrema.
 - No copiarán, distribuirán o transferirán electrónicamente o por cualquier otro medio, programas, archivos, software o manuales de propiedad o bajo licencia de la compañía sin previa autorización.

4.7. Recursos tecnológicos. [ISO/IEC 27001:2005 A.9.2]

El uso adecuado de los recursos tecnológicos asignados por Servicios Integrales a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

- La instalación de cualquier tipo de software o hardware en los equipos debe contar con la aprobación del Gerente de Operaciones y Tecnología, de acuerdo con las condiciones contractuales; por tanto, son los únicos autorizados para autorizar al equipo de soporte a realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la Gerente de Operaciones y Tecnología de Servicios Integrales.
- Ningún computador tendrá permisos de administrador. Salvo el personal de soporte técnico debidamente autorizado.
- Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. El Técnico, que describe la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman y el

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

Funcional, que describe a los usuarios del sistema la funcionalidad de cada una de las opciones del menú de la aplicación.

- La Gerente de Operaciones y Tecnología debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de Servicios Integrales; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Gerencia Tecnología de la Información.
- Todos los equipos de cómputo y equipos de comunicación como routers, switches u otros, de propiedad de Servicios Integrales, deben llevar un identificador único, legible de manera que los inventarios puedan hacerse de manera eficiente.
- El equipo especializado de cómputo que soporta la operación del negocio (servidores, enrutadores, bases de datos, etc) se instalará en lugares adecuados con excelentes condiciones de seguridad física y ambiental.
- Se debe realizar análisis por parte de la Gerencia Tecnología de la Información de todos los equipos de cómputo de la empresa con el antivirus elegido para la protección y eliminación de archivos que presenten infección con previa autorización del propietario de la información.
- La Gerente de Operaciones y Tecnología debe tener disponible el mapa actualizado de las instalaciones eléctricas y de comunicaciones de los equipos de cómputo en la red.
- Las instalaciones eléctricas y de comunicaciones deben permanecer resguardadas del paso de personas o máquinas y libres de cualquier interferencia eléctrica o magnética.
- Todo sistema computarizado multiusuario perteneciente a la empresa debe contar con un administrador de seguridad designado para definir los privilegios de los usuarios, monitorear los registros del control de acceso.

4.8. Protección contra software malicioso. [ISO/IEC 27001:2005 A.10.4]

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

Servicios Integrales establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispymware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red empresarial, en donde se cuenta con controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la Gerente de Operaciones y Tecnología autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

4.9. Copias de respaldo. [ISO/IEC 27001:2005 A.10.5]

Servicios Integrales debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Gerencia de Operaciones y Tecnología y los Centros de Producción que esta administre, contenida en la plataforma tecnológica de cada esquema implementado, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

Es responsabilidad de la Gerencia de Operaciones y Tecnología la custodia de los instaladores de programas informáticos adquiridos por la empresa o responsable de acceso a la administración de licencias, en caso de que éstos sean digitales.

4.10. Control de acceso lógico. [ISO/IEC 27001:2005 A.11.1]

- Los sistemas de información de la compañía deben contar con privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad de la información corporativa.
- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de Servicios Integrales o el Centro de Producción que este administre, debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias.
- Los responsables de la administración de la infraestructura tecnológica de Servicios Integrales asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por la Gerencia de Operaciones y Tecnología de la Información.

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

- Los usuarios que han sido autorizados para ver la información confidencial con un cierto nivel de sensibilidad pueden acceder sólo a la información de ese nivel o de grados inferiores.
- No debe otorgarse privilegios para utilizar los equipos de cómputo o los sistemas de comunicación de la empresa a las personas que no sean empleados como contratistas o consultores, a menos que se obtenga previa autorización de gerencia.

4.11. Gestión de contraseñas de usuario. [ISO/IEC 27001:2005 A.11.2.3]

- Todos los recursos de información críticos del Servicios Integrales tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por la Gerencia de Operaciones y Tecnología.
- Todo funcionario o tercero que requiera tener acceso a los sistemas de información de Servicios Integrales, debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la organización. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

4.12. Escritorio y pantalla limpia. [ISO/IEC 27001:2005 A.11.2.4]

- Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de Servicios Integrales, deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.
- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- Se recomienda no mantener ningún tipo de carpeta de archivos directamente en el escritorio de la aplicación. Solo se permitirá iconos de acceso directo a aplicaciones.

4.13. Segregación de redes. [ISO/IEC 27001:2005 A.11.4.5]

- La plataforma tecnológica de Servicios Integrales, que soporta el Software SIOT debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019

de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La Gerencia de Operaciones y Tecnología es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

- Servicios Integrales, establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Organización.

4.14. Identificación de requerimientos de seguridad. [ISO/IEC 27001:2005 A.12.1.1]

- La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en Servicios Integrales, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad de la Gerencia de Operaciones y Tecnología y las dependencias propietarias del sistema en cuestión.
- Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre Servicios Integrales y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información.

4.15 Control de vulnerabilidad técnica [ISO/IEC 27001:2005 A.12.6.1]

- Con el fin de mitigar y evitar pérdidas o daños en el código fuente se deberá realizar pruebas de caja blanca, estas permiten identificar si en la adición de código se han abierto nuevas vulnerabilidades. Estas pruebas de caja blanca deberán ejecutarse por lo menos 1 vez al año, ya sea a través de un proveedor interno o externo, esta tarea podrá ser generada por una herramienta automatizada, la cual permita la ejecución de pruebas simulando distintos valores de entrada para examinar cada uno de los posibles flujos de ejecución del software de esta manera validar que se devuelvan los valores de salida esperados. En el caso de identificar riesgos estos estarán categorizados en Críticos, Altos, Medio y Bajo, donde se dará mayor atención a los que estén categorizados como Críticos, Alto y Medio para así minimizar el impacto del ataque.

REVISÓ: DIANA MILENA CAICEDO
CARGO: LÍDER DE PROYECTO
FECHA: 21/10/2019

APROBO: NATALIA LONDOÑO GUERRA
CARGO: GERENTE DE OPERACIONES Y TI
FECHA: 21/10/2019