Industria y Comercio
SUPERINTENDENCIA

Políticas de
Seguridad de la Información

CONTENIDO

1 INTRODUCCIÓN/PRESENTACIÓN

La información es un activo fundamental en las actividades de la Superintendencia de Industria y Comercio, por lo cual siempre debe estar apropiadamente protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad, de tal manera que minimice los riesgos y asegure la continuidad del propósito misional de la Entidad.

Para la preservación de confidencialidad, integridad, disponibilidad y privacidad de la información como principios de la Seguridad de la Información, la Superintendencia de Industria y Comercio, genera e implementa las políticas descritas en este documento, en el marco del Sistema de Gestión de la Seguridad de la Información (SGSI) de la SIC y de los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones en materia de Seguridad de la Información.

2 OBJETIVO

Establecer las políticas de seguridad de la información de la Superintendencia de Industria y Comercio - SIC, con el fin de proteger la confidencialidad, integridad, disponibilidad y privacidad de la información de la Entidad.

3 ALCANCE

Las políticas definidas en el presente documento deben ser conocidas y aplicadas por todos los procesos estratégicos, misionales, apoyo y de evaluación de la Superintendencia de Industria y Comercio, así como por todos los servidores públicos, contratistas y terceros, directos e indirectos, que de una u otra manera tengan una vinculación laboral o acuerdos con la misma.

4 GLOSARIO

ACTIVO DE INFORMACIÓN: Algo que para entidad u organización tiene valor y se debe proteger como (Información Digital, Información Física, Software, Hardware, Servicio, Recurso Humano).

AMENAZA: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

CENTROS DE DATOS: Son habitaciones donde se instalan los dispositivos de comunicación y la mayoría de los cables.

CIFRAR: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

CÓDIGO MALICIOSO: programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.

COMMUNITY MANAGER: Persona que se designa para el manejo operativo de redes sociales de la Entidad.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

GTIFSD: Grupo de trabajo de informática Forense y Seguridad Digital.

HARDWARE: Parte tangible de un sistema informático, que puede corresponder a componentes de tipo: mecánico, electrónico, eléctrico, o electromecánico.

INCIDENTE DE SEGURIDAD: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORMACIÓN: Hace referencia a los datos en formato digital o físico, tratados, creados, procesados, almacenados, archivados o borrados durante la ejecución de procesos misionales de la Superintendencia de Industria y Comercio.
INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

ISO 27001: Estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la metodología del Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: Responsable o encargado de gestionar, planear, coordinar y administrar los procesos de seguridad de la información en la entidad.

OSCAE: Oficina de Servicios al Consumidor y de Apoyo Empresarial.

OTI: Oficina de Tecnología e Informática.

PARTES INTERESADAS: Son todos los grupos de interés que de alguna forma se puedan ver afectados por la actividad de Seguridad de la Información o cuyas decisiones puedan afectar al SGSI.

PROGRAMAS UTILITARIOS: Son programas diseñados para realizar una función determinada, se refiere normalmente al software que resuelve problemas relacionados con la administración del sistema del equipo de cómputo.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SIC: Superintendencia de Industria y Comercio.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SISTEMA DE INFORMACIÓN: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

TECNOLOGÍA DE LA INFORMACIÓN: Se refiere al hardware y software operados por la Entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

USUARIO: Se refiere a todo servidor público, contratista o tercero de la SIC.

VULNERABILIDAD: Es la capacidad, las condiciones y características del sistema mismo (incluyendo la Entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

VPN: Siglas en inglés de Virtual Private Network. Es una tecnología de red que permite una extensión segura de la red local (LAN), sobre una red pública o no controlada como Internet.

WIFI: Tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos, como computadoras, tablets, smartphones o celulares, etc., mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información.

WPA-PSK: Abreviatura de Wi-Fi Protected Access, es un protocolo de seguridad desarrollado por la Wi-Fi Alliance para redes inalámbricas que implementa la mayoría de secciones del estándar IEEE 802.11i. WPA hace uso de TKIP (Temporal Key Integrity Protocol) para generar una llave por cada paquete transmitido, y hace una revisión de la integridad de los mensajes a través del algoritmo Michael, el cual es más robusto que CRC (Cyclic Redundancy Check).

WPA2-PSK: Abreviatura de Wi-Fi Protected Access 2, es un protocolo que implementa las secciones obligatorias del estándar IEEE 802.11i y requiere certificación por parte de la Wi-Fi Alliance para su uso. Es considerado más robusto que WPA-PSK.

WEP: Abreviatura de Wired Equivalent Privacy, es un sistema de cifrado incluido en el estándar IEEE 802.11, que permite codificar la información que se transmite y que actúa como protocolo para redes inalámbricas. Una de sus principales debilidades es el uso de la misma llave para el cifrado de todos los paquetes transmitidos, convirtiéndolo en un protocolo vulnerable.

802.1X: Estándar de control de acceso desarrollado por el IEEE que realiza la autenticación utilizando un elemento autenticador y un servidor de autenticación, los cuales gestionan dos tipos de puertos autenticados: Puertos controlados y puertos no controlados. Para la autenticación de los clientes utiliza el protocolo Radius o Diameter.

5 RESPONSABLES

El Despacho del Superintendente de Industria y Comercio, la Secretaría General, las Delegaturas, las Direcciones, los Asesores, los Jefes de oficina, los Coordinadores, los funcionarios, contratistas y terceros son responsables de la

implementación y cumplimiento de las Políticas del Sistema de Gestión de Seguridad de la Información dentro de sus áreas.

Las Políticas del Sistema de Gestión de Seguridad de la Información es de aplicación obligatoria para todo el personal, sin importar el nivel jerárquico o su posición en el organigrama de la entidad.

6 POLÍTICAS

6.1 POLÍTICA DE ORGANIZACIÓN INTERNA

Objetivo:

Dar lineamientos para controlar la implementación y operación de la seguridad de la información dentro de la Superintendencia de Industria y Comercio.

- El Comité Institucional de Gestión y Desempeño de la SIC debe revisar y aprobar las políticas de seguridad de la información, las propuestas de implementación de medidas de seguridad de la información cuya aplicación sea de carácter transversal a la Entidad e impulsar el desarrollo de proyectos de seguridad de la información.

- El Oficial de Seguridad de la Información o a quien él delegue, debe mantener contacto con las autoridades en materia de seguridad de la información, por ejemplo, CSIRT, Colcert, CCOC. A su vez, los Coordinadores y Jefes de Oficina, de acuerdo con sus competencias, deben tener a su disposición las líneas de contacto de las empresas de servicio públicos, los servicios de emergencia, los proveedores de electricidad, de salud y seguridad, por ejemplo, bomberos (en relación con la continuidad de negocio), los proveedores de telecomunicaciones (en relación con la disponibilidad y enrutamiento de líneas) y los proveedores de suministro agua.

- El Oficial de Seguridad de la Información revisará y aprobará el plan de sensibilización en seguridad de la información en la SIC o el documento que haga sus veces.

- El Oficial de Seguridad de la Información o a quien él delegue, debe participar regularmente de los grupos de interés especial u foros de seguridad especializados y asociaciones profesionales para compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.

- El Oficial de Seguridad de la Información o a quien él delegue, debe verificar y gestionar el cumplimiento de las políticas de seguridad de la información.

- El Oficial de Seguridad de la Información o a quien él delegue, debe revisar las políticas para la seguridad de la información a intervalos planificados o si ocurren cambios significativos.

6.2 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

Objetivo:

La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.

- Se debe integrar la seguridad de la información en la gestión de los proyectos de la SIC, independientemente de su naturaleza, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. La identificación de riesgos de seguridad de la información en proyectos, de ser requerido puede ser asesorada por el Oficial de Seguridad de la Información o a quien él delegue, para lo cual se debe tener en cuenta:

    - Que los objetivos del proyecto no vayan en contravía de la política de seguridad de la información.
    - Que la valoración de los riesgos de seguridad de la información e identificación de los controles necesario se lleve a cabo en una etapa temprana del proyecto.
    - Que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

6.3 POLÍTICA DE SEGURIDAD PARA EL TELETRABAJO

Objetivo:

Proteger la información institucional en un entorno de teletrabajo.

- El teletrabajador deberá resguardar la información institucional, impidiendo el acceso a terceras personas, en consecuencia, el acceso a los sistemas de información de la SIC será efectuado siempre y en todo momento bajo el control y responsabilidad del teletrabajador, siguiendo los procedimientos establecidos por la Entidad.

- El teletrabajador debe utilizar la información, incluyendo los datos de carácter personal a los que tenga acceso, única y exclusivamente para cumplir con sus funciones u obligaciones con la Entidad.

- El acceso de los teletrabajadores a los sistemas de información de la Entidad, se debe realizar a través de la VPN autorizada por la Oficina de Tecnología e Informática.

- El teletrabajador debe cumplir con las medidas de seguridad que la Entidad ha definido para asegurar la confidencialidad, secreto e integridad de la información, incluyendo los datos de carácter personal a los que tenga acceso.

- El teletrabajador no debe ceder la información en ningún caso a terceras personas, incluyendo los datos de carácter personal a los que tenga acceso, ni siquiera a efectos de su conservación.

- El teletrabajador no debe brindar acceso al equipo de cómputo de la Entidad, a la información o a los recursos, a personas cercanas, por ejemplo, familia y amigos.

- En el caso de utilizar una red inalámbrica para la conexión, ésta debe cumplir con la política uso de redes inalámbricas en cuanto al tipo y esquema de seguridad (cifrado).

6.4 POLÍTICA SEGURIDAD DEL RECURSO HUMANO

Objetivo:

Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

6.4.1 Control antes de asumir el empleo

- El Grupo de Administración de Personal y el Grupo de Contratación deben verificar los antecedentes de todos los candidatos a servidor público o contratista de acuerdo con las leyes vigentes, reglamentos y ética pertinentes.

- Cuando un individuo es contratado para un rol de Seguridad de la Información específico, la Oficina de Tecnología e Informática debe asegurar que el candidato:

  - Tenga la competencia necesaria para desempeñar el rol.
  - Sea confiable para desempeñar el rol.

6.4.2 Términos y condiciones del empleo

- Todos los servidores públicos y contratistas que requieran acceso a la información de la Entidad, deberán aceptar el acuerdo de confidencialidad, antes de tener acceso a la misma.

- El Grupo de Contratación y el Coordinador del Grupo de Trabajo de Administración de Personal, deben asegurar que los servidores públicos y/o contratistas acepten los términos y condiciones relativos a la Seguridad de la Información, referente a la naturaleza y al alcance del acceso que tendrán a los activos de la Entidad asociados con los sistemas y servicios de información, definiendo:

  - Las responsabilidades y derechos legales, por ejemplo, con relación a leyes sobre derecho de autor o legislación sobre protección de datos.
  - Las responsabilidades del servidor público o contratista para el manejo de la información recibida de otras compañías o partes externas.
  - Las acciones por tomar, si el servidor público o contratista no tiene en cuenta los requisitos de seguridad de la Entidad.

6.4.3 Durante la ejecución del empleo

- Los Coordinadores, Jefes de Oficina, Delegados, Directores y Alta dirección deben exigir a todos los servidores públicos, contratistas y terceros la aplicación de la Seguridad de la Información de acuerdo con las políticas y procedimientos establecidos por la Entidad.

- Todos los servidores públicos y contratistas periódicamente deben recibir sensibilización en seguridad de la información, así como actualizaciones regulares sobre las políticas y procedimientos de la Entidad con respecto a la Seguridad de la Información. Para lo cual, el Oficial de Seguridad de la Información será responsable del contenido de la sensibilización, el Grupo de Desarrollo del Talento Humano incentivará la participación de los usuarios y la Oficina de Servicios al Consumidor y Apoyo Empresarial apoyará el diseño de las piezas gráficas que se requieran.

- El Grupo de Trabajo de Informática Forense y Seguridad Digital deberá participar anualmente en al menos un evento de simulación nacional o internacional para desarrollar, habilidades, destrezas en materia de seguridad digital.

6.4.4 Terminación y cambio de empleo

- El Coordinador del Administración de Personal y el Coordinador del Grupo de Contratación deben definir procedimientos para asegurar que la información institucional permanezca en custodia de la Entidad, cuando se retire un servidor público o se termine la vinculación contractual con los contratistas. En todo caso todo servidor público y contratista debe facilitar a su jefe inmediato o supervisor de contrato, según sea el caso, toda la información que se encuentre a su cargo.

- El Grupo de Administración de Personal y el Grupo de Contratación deben dar a conocer a los servidores públicos y contratistas las responsabilidades con respecto a los requisitos de seguridad de la información, el acuerdo de seguridad de la información, y las responsabilidades legales vigentes en el momento de la terminación laboral o contractual.

- Para efectos del bloqueo de los accesos a las instalaciones y a los sistemas de información de la Entidad, el Grupo de Administración de Personal y el Grupo de Contratación informarán a la mesa de servicios, administrada por la Oficina de Tecnología e Informática y al Grupo de Servicios Administrativos y Recursos Físicos acerca de la desvinculación de personal o cambios de dependencias. En consecuencia, se deben eliminar todos los accesos del servidor público y/o contratista que ha terminado su vinculación laboral con la Entidad, a saber:

  - Eliminación del acceso a los sistemas de información.
  - Eliminación de los datos personales y/o biométricos de los sistemas de control de acceso.
  - Desactivación del carnet o cualquier medio de autenticación, que lo acredita como servidor público o contratista de la SIC y retiro inmediato del mismo.
  - Informar a los proveedores y demás personal con el que el servidor público o contratista tenga contacto, indicándole que esa persona ya no labora en la SIC y quién asumirá sus funciones o responsabilidades.

6.4.5 Proceso disciplinario

- Servidores públicos que incumplan y/o violen las políticas de la Seguridad de la Información de la SIC, se les aplicará lo establecido en la ley del Código Único Disciplinario (Ley 1952 de 2019), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las reglamenten o complementen.

- Los contratistas que incumplan y/o violen las políticas de la Seguridad de la Información de la SIC pueden ser reportados ante la procuraduría y/o Entidades competentes, según sea el caso.

6.5 POLÍTICA DE USO ACEPTABLE DE ACTIVOS

Objetivo:

Los usuarios de la Superintendencia de Industria y Comercio se responsabilizan de gestionar de una forma adecuada los activos de información de los cuales son responsables o custodios.

- Por ningún motivo un servidor público y/o contratista puede utilizar los activos de información de la SIC para almacenar, transmitir o generar información personal.

- Todos los requerimientos asociados a los recursos tecnológicos deberán ser solicitados a través de la mesa de servicios con su respectiva justificación para su viabilidad.

- Solo los líderes de proceso están autorizados a remitir a la mesa de servicios, la solicitud para habilitar los accesos a los recursos informáticos y tecnológicos, identificando el usuario (interno o externo), relacionando los servicios que requiera y el tiempo si es requerido. Así mismo, deben especificar el tipo de acceso (lectura, escritura, modificación y borrado) y los roles sobre carpetas compartidas.

- Las salas de audiencia o video-conferencia (salas de facilitación virtual) deben ser de uso exclusivo para temas laborales de la SIC.

- La OTI a través de la Coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá implementar una solución tecnológica que permita el monitoreo y detección de los aplicativos instalados en la infraestructura tecnológica de la SIC.

- La extracción, préstamo, copia, venta y/o renta de software corporativo para fines externos y/o personales, no está autorizado bajo ninguna circunstancia.

6.5.1 Uso de internet

- Todos los accesos a internet de los equipos de cómputo institucionales deben ser realizados a través de los canales de acceso provistos por la Entidad. En caso de necesitar una conexión a internet especial, ésta debe ser notificada y aprobada por el Jefe de la OTI.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, es responsable de asegurar los servicios de internet permitidos en la Entidad.

- El uso de internet debe estar destinado exclusivamente a la ejecución de las actividades laborales de la SIC.

- Salvo situaciones justificadas y aprobadas por la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, no está permitida la conexión a dominios de internet que generen tráfico de broadcast (audio o video) por fuera de los dominios institucionales de la SIC.

- Los usuarios no deben acceder a páginas clasificadas con contenido pornográfico o no permitidas.

- Los usuarios no deben instalar software que permita acceder a páginas o servicios no autorizados, por ejemplo, aplicaciones P2P (Ares o Emule).

- Se permite el acceso a redes sociales solamente en los siguientes horarios:

    - Entre las 00:00 h y las 8:00 h
    - Entre las 12:00 h y las 14:00 h
    - Entre las 17:00 h y las 00:00 h

6.5.2 Uso de intranet (Intrasic)

- Los usuarios no deben re-direccionar información que aparezca en intranet a terceros sin autorización de la SIC.

- La información que se publique en la intranet de la SIC, debe contar con la aprobación del líder de proceso responsable, según el tema.

- Es responsabilidad de la Oficina de Servicios al Consumidor y Apoyo Empresarial revisar, aprobar y depurar la información publicada. De acuerdo a los procedimientos establecidos en el Grupo de Trabajo de Comunicación CS03-P01 Procedimiento de Comunicación.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe gestionar que la SIC cuente con la infraestructura tecnológica adecuada para la plataforma que soporta la intranet.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe implementar los controles necesarios para asegurar el adecuado acceso de la intranet.

6.5.3 Uso de dispositivos móviles institucionales

Todos los usuarios que tengan a su cargo dispositivos móviles institucionales deben hacer uso adecuado y responsable de los mismos y proteger de terceros el acceso a los servicios de la SIC.

- Los dispositivos móviles institucionales que lo permitan, deben tener sus unidades de almacenamiento cifradas para evitar la pérdida de confidencialidad de la información en caso de pérdida o robo del dispositivo.

- En caso de robo o pérdida de un dispositivo móvil institucional, el coordinador del Grupo de Trabajo de Servicios Tecnológicos delegará a quien debe realizar el borrado remoto de la información almacenada en el dispositivo con el fin de evitar que la información quede expuesta a terceros no autorizados.

- Quienes tengan asignados dispositivos móviles institucionales, no deben modificar las configuraciones de seguridad de los mismos ni desinstalar el software provisto por la Entidad.

- Quienes tengan asignados dispositivos móviles institucionales, deben evitar la instalación de programas desde fuentes externas y/o de procedencia desconocida.

- Todo dispositivo móvil institucional debe tener un esquema de autenticación y desbloqueo, como por ejemplo autenticación por contraseña o patrón de movimiento.

- Quienes tengan asignados dispositivos móviles institucionales, deben evitar conectarlos por puerto USB a cualquier computador público, o redes WIFI-Públicas de hoteles o cafés internet, entre otros.

- Quienes tengan asignados dispositivos móviles institucionales, no deben almacenar videos, fotografías o información personal en los mismos.

- Cualquier servidor público, contratista o terceros directos o indirectos que requiera acceder a los servicios de la SIC desde su(s) dispositivo(s) móvil(es) institucional(es) (correo electrónico, servicio de almacenamiento en la nube, calendario, entre otros), tiene la responsabilidad de proteger la información contra el acceso y divulgación no autorizada, para lo cual, al menos debe:

    - Trabajar con versiones de software actualizadas y de uso legal.
    - Tener contraseña de ingreso o patrón de bloqueo del equipo.

- Tener instalado un antivirus.

- La Oficina de Tecnología e Informática podrá borrar todos los datos del dispositivo móvil o acceder a la ubicación del dispositivo móvil de forma remota, siempre y cuando exista una solicitud escrita del propietario o responsable del dispositivo debidamente justificada (memorando o e-mail).

- La Oficina de Tecnología e Informática podrá eliminar la cuenta institucional del dispositivo móvil de forma remota, cuando se identifique el incumplimiento de cualquiera de las políticas de seguridad de la información de la SIC o finalice la relación laboral o contractual con la Entidad.

6.5.4 Uso de dispositivos móviles personales

El uso de los dispositivos móviles personales utilizados por los funcionarios, contratistas y aliados estratégicos y que no son de propiedad de la Entidad, por medio de los cuales consultan, revisan, modifican, transmiten y/o almacenan información de la Entidad, deben aplicar las configuraciones de seguridad obligatorias y necesarias antes de tener cualquier acceso a recursos de red de la Entidad y/o activos de información.

- El acceso remoto seguro se controla estrictamente con cifrado a través de redes privadas virtuales (VPN).
- Los usuarios autorizados deben proteger su nombre de usuario y contraseña, incluso de sus familiares.

- Los usuarios autorizados deben asegurar que el host remoto no esté conectado a ninguna otra red al mismo tiempo, con la excepción de las redes personales que están bajo su control total o bajo el control completo de un usuario o de un tercero autorizado.

- Cada usuario es responsable por cualquier uso indebido de la información de la SIC accedida desde sus dispositivos personales.

- Cualquier servidor público o contratista que requiera acceder a los servicios de la SIC desde su equipo de cómputo, portátil o tableta personal (correo electrónico, servicio de almacenamiento en la nube, calendario, entre otros), tiene la responsabilidad de proteger la información contra el acceso y divulgación no autorizada, para lo cual, al menos debe cumplir con las siguientes condiciones:

  - Tener un software antivirus validado y autorizado por la Entidad; donde se valide esquema de actualizaciones de firmas, módulos de seguridad activados y programación de escaneos periódicos.

- Garantizar que los dispositivos estén protegidos con contraseñas o patrones de bloqueo, se recomienda activar un doble factor de autenticación (MFA).
- Se debe validar el estado de las actualizaciones del sistema operativo.
- Es responsabilidad del dueño tomar nota del IMEI para solicitar su anulación en caso de pérdida.
- En el caso de almacenar información clasificada como información pública reservada y/o Información pública clasifica y/o información no clasificada en el dispositivo móvil, el responsable de ese dispositivo deberá garantizar un esquema de cifrado y disponibilidad de la información en caso de pérdida, autorizado por la entidad.
- Los dueños de los dispositivos móviles aceptan los controles definidos dentro de sus dispositivos, en los cuales la Entidad ante pérdida o venta de estos, pueda ejecutar acciones de mitigación de riesgos asociados, sobre la información contenida y de propiedad de la SIC en estos dispositivos.

- Los dispositivos móviles contarán con los métodos de autenticación establecidos y/o validados por la Entidad.

- En el caso de presentar pérdida del dispositivo móvil, se deberá seguir el procedimiento de gestión de incidentes de la Entidad, con el objetivo de garantizar los controles correctivos definidos para ese tipo de incidente, ejemplo: bloqueo de los accesos a los sistemas de información, cambio de claves, borrado de información remota, etc.

6.5.5 Uso del correo electrónico institucional

- El servicio de correo electrónico institucional es una herramienta para el intercambio de información exclusivamente laboral, por lo tanto, las cuentas deben ser otorgadas únicamente a servidores públicos y contratistas de la Entidad que lo requieran.

- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la SIC cuenta con el dominio @sic.gov.co.

- Las cuentas de correo electrónico institucional son creadas para el uso exclusivo de las funciones u obligaciones de los servidores públicos y contratistas, por lo tanto, deben actuar siempre con criterios de racionalidad, respeto y seguridad de la información.

- Los servidores públicos y contratistas son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.

- Se prohíbe el uso de correos personales con el fin de establecer o transferir información institucional.

- El usuario del correo electrónico se compromete a reportar oportunamente a la mesa de servicios cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, perdida de contraseñas, etc.

- Todo correo de procedencia sospechosa o correos no deseados, deben ser ignorados y reportados a la mesa de servicios, con el fin de evitar posibles infecciones por virus o código malicioso.

- Se debe evitar el envío de cualquier información ajena a las labores propias del cargo, es decir, el correo electrónico institucional no puede ser utilizado para fines personales, comerciales y/o económicos.

- Se prohíbe usar el correo institucional para la propagación de correos con mensajes cadena, mensajes publicitarios, imágenes o videos que contengan contenidos ofensivos, material sexual, de intimidación, con contenidos ilegales o de discriminación de género, nacionalidad, religión, raza, orientación política o discapacidad.

- En ningún caso está permitido compartir contactos o listas de distribución de la SIC con personal externo.

- No se podrá incluir mensajes de correo electrónico con contenidos que comprometan el buen nombre de la SIC, instituciones o personas.

- Se debe evitar la distribución de software o contenidos que violen la propiedad intelectual o derechos de autor.

- Las listas de distribución internas sólo podrán ser utilizadas para cumplir los fines de comunicación e información interna, mas no para fines diferentes a los del cumplimiento de los objetivos de la SIC.

- Los usuarios no podrán alterar la información existente en un correo electrónico cuando en una respuesta se incluya el mensaje original.

- Los mensajes enviados por correo electrónico no se deben imprimir de modo que se evita el uso de papel, excepto si la impresión es necesaria para fines laborales y se puedan almacenar de forma segura.

- Quien incurra en violación de las políticas de uso del correo electrónico, será objeto de la debida investigación disciplinaria a que haya lugar.

- Cada mensaje electrónico debe incluir el fondo y la firma oficializada por la SIC.

- Todos los adjuntos al correo electrónico deben ser revisados por el antivirus con el que cuenta la SIC.

6.5.6 Correos electrónicos masivos

- La Oficina de Servicios al Consumidor y Apoyo Empresarial y los niveles Directivos Superiores (Superintendente y Secretaría General) son los encargados de autorizar a funcionarios, contratistas o terceros el envío de correos masivos, por medio de las listas de distribución creadas en la Entidad para tal fin. En este sentido, dichas dependencias son las únicas acreditadas para realizar la mencionada solicitud a la mesa de servicios, la cual debe indicar el nombre del usuario autorizado, la cuenta de correo autorizada y el periodo que se requiere mantener dicho permiso.

6.5.7 Autenticación Doble Factor Correo Electrónico

- Los usuarios tanto funcionarios como contratistas y demás colaboradores de la SIC, deben activar/habilitar la autenticación doble factor para acceso al correo electrónico institucional.

6.5.8 Manejo de redes sociales

- El uso de redes sociales institucionales, tales como Facebook, Twitter, Instagram, YouTube, LinkedIn, Flickr, entre otros, deben seguir lo dispuesto en la circular interna No. 15 del 2019. El uso o manejo de redes sociales se debe realizar de acuerdo con lo estipulado en el CS03-P01 Procedimiento de Comunicación y protocolos establecidos desde la OSCAE.

6.5.9 Uso de redes inalámbricas

- Se debe contar con mecanismos de control de acceso lógico para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes inalámbricas, como métodos de autenticación que eviten accesos no autorizados.

- Para las conexiones a redes inalámbricas, solo se deben permitir esquemas de seguridad que provean confidencialidad de la información de usuario transferida sobre medios inalámbricos y autenticación para dispositivos compatibles con el estándar IEEE 802.11. Al momento de elaboración de este documento los siguientes esquemas de seguridad son válidos y proveen confidencialidad y autenticación sobre medios inalámbricos para dispositivos IEEE 802.11: WPA-PSK, WPA2-PSK y 802.1X. En ninguna circunstancia se debe usar WEP.

- La mesa de servicios de la OTI es responsable de mantener en operación la infraestructura que proporciona red inalámbrica.

- El usuario se compromete a hacer uso productivo y seguro de la red inalámbrica.

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público.

- Quienes tengan asignados dispositivos móviles institucionales, deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los mismos.

- Los usuarios deben reportar a la mesa de servicios de la OTI, incidentes o errores que se presenten durante el uso de los servicios de red inalámbrica.

- En caso de que una persona externa requiera del servicio de la red inalámbrica, es responsabilidad del servidor público, comunicarle las políticas de uso de la red.

- La SIC a través de la OTI, debe disponer para los visitantes el servicio de acceso a internet, a través de la red inalámbrica "Zona Wifi GRATIS para la gente", durante los horarios de atención al público previstos por la SIC. En caso de que la conexión deba suspenderse, se indicará a los usuarios, señalando igualmente la fecha y hora a partir de la cual se reanudará la conexión.

- La red inalámbrica "Zona Wifi GRATIS para la gente" debe estar aislada de la red de datos principal de la SIC, brindando únicamente el servicio de internet, permitiendo únicamente el contenido aprobado en las políticas de seguridad de la SIC.

6.5.10 Uso del servicio de nube

- Los servidores públicos o contratistas no tienen permitido almacenar información de la SIC en servicios de alojamiento de archivos multiplataforma en la nube (Dropbox, Box, Bitcasa, Mesa, icloud, entre otros similares) que no hayan sido autorizados por la OTI.

- Cuando se contraten servicios tecnológicos en la nube, la OTI deberá asegurar el establecimiento de cláusulas contractuales y procedimientos para la protección de la información, definiendo, entre otros, métodos seguros de trasferencia de información, cumplimiento de los lineamientos estipulados en la Cartilla - Protección de los Datos Personales en los servicios de computación en la nube (Cloud Computing) emitida por la SIC, mecanismo fuertes de autenticación, cifrado de información, devolución y borrado seguro de información, acuerdos para la confidencialidad, integridad y disponibilidad de

información. Adicionalmente deberá asegurar que el proveedor de servicios en la nube realice gestión sobre la ciberseguridad.

- El acceso a las nubes contratadas por la Entidad, debe contar con doble factor de autenticación (MFA) habilitado para los usuarios (funcionario y/o contratistas terceros directos o indirectos) autorizados.

6.6 RESPONSABILIDADES SOBRE LOS ACTIVOS

Objetivo:

Identificar los activos de información de todos los procesos de la Superintendencia de Industria y Comercio, y a su respectivo propietario, es decir, quien tenga la responsabilidad delegada sobre la gestión para controlar todo el ciclo de vida de un activo.

- La OTI a través de la coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, desarrollará una guía para el levantamiento de los activos de información de la SIC.

- La OTI a través de la coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, actualizará el inventario de activos de información de la SIC periódicamente, o cuando se realiza actualizaciones al proceso al que pertenece el activo.

- Los Lideres de los procesos de la SIC, son los responsables de identificar y mantener actualizados los activos de información que requieren de mayor protección para el cumplimiento misional de la Entidad, con el apoyo de la OTI a través de la Coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces.

6.7 POLÍTICA DE DEVOLUCIÓN DE ACTIVOS DE INFORMACIÓN

Objetivo:

Todos los servidores públicos, contratistas, terceros directos o indirectos deberán devolver todos los activos de la Superintendencia de Industria y Comercio a su cargo, al terminar su empleo, contrato o acuerdo.

- El inventario de la infraestructura computacional (equipos centrales, computadores de escritorio, software, impresoras, escáneres y equipos multifuncionales) está a cargo de la Dirección Administrativa.

- Todos los servidores públicos, contratistas, terceros directos o indirectos de la SIC en el momento de su desvinculación, deberán devolver todos los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación, al jefe inmediato o supervisor del contrato.

- Todos los servidores públicos, contratistas, terceros directos o indirectos de la SIC, deberán solicitar a la mesa de servicios realizar un backup de la información contenida en los equipos informáticos antes de la devolución de los activos.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe realizar el procedimiento de borrado seguro a los equipos informáticos devueltos, con el fin de evitar que la información contenida pueda ser recuperada.

- En el momento de cambio de labores de los servidores públicos a otras áreas, éstos deben realizar la entrega de su puesto de trabajo al jefe inmediato o supervisor; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

- Cuando se asigne un equipo de cómputo a un servidor público, contratista, terceros directos o indirectos, se debe asegurar que no contenga información de otros colaboradores.

6.8 POLÍTICA DE GESTIÓN DE MEDIOS REMOVIBLES

Objetivo:

Implementar procedimientos para la gestión de medios removibles de la Superintendencia de Industria y Comercio, de modo que se evite la divulgación, modificación, retiro, destrucción no autorizada de la información que se encuentra almacenada en medios físicos.

- El contenido de medios removibles (cintas, discos, discos flash, discos duros, discos compactos, DVDs, unidades de almacenamiento USB, cámaras fotográficas, cámaras de video, teléfonos celulares, entre otros) que se dejarán de utilizar, deben pasar por un proceso que los haga irrecuperables (Ver numeral 6.28 Política de borrado seguro).

- La Dirección Administrativa debe tener un registro de los medios removibles institucionales.

- Los medios removibles deben almacenarse en un ambiente protegido y seguro, siguiendo las recomendaciones de disposición y almacenamiento del fabricante.

- La información de carácter sensible que se disponga en un medio extraíble debe seguir un proceso de cifrado adecuado (Ver numeral 6.12 Política de controles de cifrado). La solicitud para realizar el cifrado se realizará por medio de la mesa de servicios.

- Todos los medios removibles conectados a equipos informáticos deben seguir un proceso de análisis y búsqueda de código malicioso adecuado. (Ver numeral 6.19 Política de control de código malicioso en este documento).

- Cuando se libera la información sensible almacenada en medios removibles, institucionales, éste se debe formatear, realizando la solicitud a la mesa de servicios.

- En caso de presentarse acceso físico y/o lógico no autorizado, daños, perdida de información o extravío del medio removible, se debe informar a la mesa de servicios, de acuerdo con lo descrito en el Procedimiento de gestión de incidentes de seguridad SC05-P01.

- Se prohíbe el uso de medios removibles institucionales, en lugares de acceso al público.

- Es responsabilidad del usuario no exponer los medios removibles institucionales a condiciones ambientales, tales como, exposición al calor, humedad, etc., que puedan afectar su buen funcionamiento.

- El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo.

6.9 POLÍTICA DE CONTROL DE ACCESO

Objetivo:

Determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para los roles de usuario específicos con relación a los activos, con la cantidad de detalle y severidad de los controles, que reflejen los riesgos de seguridad de la información asociados.

6.9.1 Control de acceso lógico y gestión de privilegios

- Se debe seguir un procedimiento formal para la creación y aprobación de cuentas de usuario. (Ver el documento procedimiento de gestión de accesos).

- Cada usuario de un sistema de información o de un acceso de teletrabajo debe disponer de una identificación única (ID) que permita determinar los responsables de una acción operativa. Sólo se permiten identificadores de grupo cuando se justifican por razones operativas y bajo aprobación por parte del Oficial de Seguridad de la Información. Por ningún motivo se deben crear cuentas de usuario genéricas.

- Se debe mantener un registro formal de todos los usuarios autorizados de un sistema de información o de un acceso de teletrabajo y se debe verificar dicho registro periódicamente.

- Se debe tener un registro de todos los niveles de acceso asignados a usuarios para los sistemas de información o de un acceso de teletrabajo.

- El otorgamiento de un determinado nivel de acceso a un servidor público o aplicativo en un sistema de información o de un acceso de teletrabajo debe ser autorizado previamente por el líder del proceso del aplicativo, siempre partiendo del principio de que se debe autorizar el mínimo nivel de privilegios necesarios para la realización de las funciones del servidor público o el funcionamiento del aplicativo.

- En caso de que un servidor público sea retirado o reasignado en sus funciones, el Grupo de Talento Humano debe informar a la mesa de servicios vía correo electrónico.

- En los casos en los que el otorgamiento de acceso se lleve a cabo por medio de una asignación de contraseña, se debe consultar la política de contraseñas (Ver numeral 6.10 en este documento).

- En el caso de que un activo de información aumente su nivel de criticidad, se deberá realizar una revisión de los usuarios que acceden a él y los privilegios de dichos usuarios para determinar su vigencia.

- Los usuarios no deben tener permisos de administrador en sus equipos de cómputo, salvo en casos debidamente autorizados por la Jefatura de la Oficina de Tecnología e Informática o la Coordinación del Grupo de Trabajo de Servicios Tecnológicos. En todo caso, los usuarios que cuenten con este permiso se comprometen a diligenciar el formato GS01-F22 - Acta de responsabilidad de

privilegios de administrador local en equipo de cómputo y a dar cumplimiento a las políticas de seguridad de la información de la SIC. Por ningún motivo deben instalar software que no haya sido adquirido oficial y legalmente por la Entidad, de acuerdo con lo establecido en el numeral 6.31 - derechos de propiedad intelectual y 6.5 - política de uso aceptable de activos del presente documento, siendo responsables en caso de incumplimiento de las mismas.

6.9.2 Gestión de usuarios conforme a las novedades de personal SIC.

- Se debe hacer el bloqueo de las cuentas de usuario y de correo electrónico institucional de los servidores públicos, durante la ejecución de algún periodo tiempo que presente alguna de las novedades administrativas definidas por la SIC, como (vacaciones, retiros, permisos, etc.), teniendo en cuenta los lineamientos establecidos por el proceso GT02 Administración, Gestión y Desarrollo del Talento Humano.

- Se debe hacer el bloqueo de las cuentas de usuario y de correo electrónico institucional de los contratistas, terceros, directos o indirectos, en caso de que el contrato presente alguna novedad contractual, tal como (terminación anticipada del contrato, suspensión del contrato, etc.). Para esto cada líder de proceso y/o supervisor del contrato, debe informar al centro de servicios integrados de TI, a fin de bloquear inmediatamente los niveles de acceso que le hayan sido otorgados.

6.10 POLÍTICA DE CONTRASEÑAS

Objetivo:

Asegurar la debida autenticación de los usuarios y controlar el acceso a los activos de información de la Superintendencia de Industria y Comercio, a través de mecanismos para la gestión, selección y uso de contraseñas.

6.10.1 Contraseñas de usuario

- En el momento de la asignación de un usuario y contraseña a una persona bien sea servidores públicos, contratista, tercero directo o indirecto o grupo de personas según la gestión, la mesa de servicios debe informar a los mismos sobre el carácter confidencial de ésta.

- Los usuarios y contraseñas se deben distribuir de forma segura, nunca mediante sistemas de transporte no cifrado (texto claro).

- Los usuarios y contraseñas no se deben almacenar en un computador en formato no cifrado.

- Las contraseñas por defecto asociadas a una herramienta de software, sistema de información o plataforma de gestión para la Superintendencia de Industria y Comercio, deben ser cambiadas inmediatamente después de la instalación.

6.10.2 Selección y uso de contraseñas

- Todos los servidores públicos, contratistas, y/o terceros directos o indirectos, antes de acceder a un recurso de tecnología de la Superintendencia de Industria y Comercio, tienen que identificarse y autenticarse por medio del usuario y contraseña que le fue asignado.

- Todos los servidores públicos, contratistas y/o terceros directos o indirectos son responsables del uso de los usuarios y contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos.

- Los servidores públicos, contratistas y/o terceros directos o indirectos, deben mantener la confidencialidad de las contraseñas.

- Los servidores públicos, contratistas y/o terceros directos o indirectos, no deben mantener registros de los usuarios y contraseñas (hojas de papel, archivos digitales, notas adhesivas post-it, etc.), a menos de que sea un método de almacenamiento aprobado por el Oficial de Seguridad de la Información.

- Los usuarios deben cambiar la contraseña siempre que haya indicio o sospecha de la puesta en peligro (acceso no autorizado) del sistema de información, herramienta de software o plataforma de gestión para la Superintendencia de Industria y Comercio, se debe hacer el cambio de contraseña a intervalos regulares, evitando la reutilización de contraseñas antiguas.

- Los servidores públicos, contratistas y/o terceros directos o indirectos, deben seleccionar contraseñas con un mínimo de ocho (8) caracteres, asimismo para las cuentas de servicio de correo electrónico deben seleccionar contraseñas con un mínimo de diez (10) caracteres con las siguientes características:

  • Debe ser alfanumérica (que contenga números, letras mayúsculas y minúsculas).

  • Debe contener caracteres especiales (#$%@/)

- Los servidores públicos, contratistas y/o terceros directos o indirectos, no deben almacenar los usuarios y contraseñas en un proceso de registro automatizado (plugin, extensión, macro, etc.).

- Los servidores públicos, contratistas y/o terceros directos o indirectos, no deben compartir usuarios ni contraseñas. El usuario y la contraseña son personales e intransferibles.

- Los servidores públicos, contratistas y/o terceros directos o indirectos no deben usar los mismos usuarios y contraseñas para propósitos de negocio o propósitos de índole personal.

- Los usuarios no deben crear contraseñas que tengan relación con el nombre propio, familiares, cargo de trabajo, etc.

6.10.3 Gestión de contraseñas

- Se debe permitir a los usuarios la elección y el cambio de sus contraseñas.

- Se debe forzar al usuario a una elección de contraseñas de calidad (ver numeral 6.10.2).

- La contraseña debe cambiarse obligatoriamente cada 45 días, o cuando lo establezca el jefe de la Oficina de Tecnología e Informática (OTI), y ésta debe ser distinta a las últimas 5 utilizadas.

- La contraseña para las cuentas de servicio de correo electrónico, debe cambiarse obligatoriamente cada 90 días o cuando lo establezca el jefe de la Oficina de Tecnología e Informática (OTI) y ésta debe ser distinta a las últimas 5 utilizadas.

- El sistema para la gestión de contraseñas debe mantener un registro de las cinco (5) contraseñas previas, utilizadas por un usuario y evitar su reutilización.

- Después de 5 (cinco) intentos no exitosos de ingreso de la contraseña, el usuario será bloqueado de manera inmediata y deberá solicitar el desbloqueo a través de la mesa de servicios.

- No deben ser visibles las contraseñas en pantalla, en el momento del ingreso, se deben utilizar caracteres de enmascaramiento.

- Las contraseñas se deben almacenar haciendo uso de cifrado en una sola vía y transmitir en formatos protegidos (cifrados).

- Se debe desactivar la opción de autoguardado de contraseñas en los diferentes navegadores web.

- Los agentes de la mesa de servicios que realizan cambios de contraseñas o crean contraseñas temporales a los usuarios de dominio de los servidores públicos, contratistas y/o terceros directos o indirectos de la Entidad, deben crear contraseñas de calidad (ver numeral 6.10.2) y evitar totalmente usar contraseñas por defecto como (“mayo2020”) durante la atención a los usuarios, para lo anterior se puede hacer uso de herramientas generadoras de contraseñas.

6.11 POLÍTICA CONTROL DE ACCESO A CÓDIGOS FUENTE DE PROGRAMA

Objetivo:

Proporcionar los lineamientos para el acceso a los códigos fuente de los programas.

- Solamente los ingenieros desarrolladores y de soporte de la OTI, podrán contar con acceso a los códigos fuente de los programas o sistemas de información y harán uso de los mismos únicamente para el cumplimiento de sus funciones u obligaciones contractuales.

- La OTI a través de la coordinación del Grupo de Trabajo de Sistemas de Información y de la coordinación del Grupo de Trabajo de Proyectos Informáticos, debe asegurar la protección de los archivos de programas fuente de los sistemas de información o software, tanto adquiridos como desarrollados al interior de la SIC.

- Los programas de código fuente de los sistemas de información y desarrollos de software de la SIC, se deben encontrar en repositorios con acceso controlado y restricción de privilegios y, se deben registrar todos los accesos a dichos programas de código fuente.

- La OTI a través de la coordinación del Grupo de Trabajo de Sistemas de Información y del coordinador del Grupo de Trabajo de Proyectos Informáticos debe llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).

- Los desarrolladores de la OTI deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los servidores públicos, contratistas ni terceros.

6.12 POLÍTICA DE CONTROLES DE CIFRADO

Objetivo:

Proporcionar los lineamientos para proteger la confidencialidad, disponibilidad e integridad de la información digital de la Superintendencia de Industria y Comercio por medio del uso adecuado de controles criptográficos.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe promover mecanismos de cifrado para la protección de información sensible transportada en computadores portátiles o medios de almacenamiento extraíble o a través de líneas de comunicación. (Ver el documento GS01-I29 Instructivo de cifrado de información).

- El coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, es el encargado de administrar la gestión de claves de cifrado, lo cual incluye su generación, distribución y revocación.

- El coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, es el encargado de gestionar que los equipos de cómputo de servidores públicos, contratistas, tercero directo o indirecto, que se encuentre en teletrabajo o aquellos que por el ejercicio de sus funciones deben hacer uso de este fuera de la Entidad, cuente con cifrado lógico mediante las herramientas tecnológicas con las que cuente la SIC.

- El coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe proteger físicamente los equipos usados para generar, almacenar y archivar las claves de cifrado.

- Se deben revocar las claves de cifrado, por ejemplo, cuando la seguridad de las claves haya estado comprometida, o cuando un usuario deja la Entidad (en cuyo caso las claves también se deberán archivar).

- Se debe mantener un registro de las operaciones de gestión de claves de cifrado (claves generadas, distribuidas y revocadas), al igual que del propietario de las claves y del tiempo de validez.

- La clave de cifrado privada de un modelo de criptografía simétrica, debe ser distribuida de forma segura al usuario o equipo para el cual se creó. No se debe usar nunca un medio de distribución no cifrado (texto plano).

- La OTI a través de sus coordinaciones deben establecer y proteger adecuadamente los sistemas de información internos y externos de la Superintendencia de Industria y Comercio, utilizando conexiones seguras en todas las aplicaciones, a través de uso de certificados SSL, (HTTPS para la confianza de usuarios) y el cifrado en la estructura de las peticiones para portales transaccionales y evitar la manipulación de parámetros en las peticiones.

6.13 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo:

Proteger las áreas que contienen información y/o servicios de procesamiento de información de la Superintendencia de Industria y Comercio.

6.13.1 Control de acceso físico

- El ingreso a las instalaciones de la Superintendencia de Industria y Comercio debe estar restringido únicamente al personal autorizado.

- El ingreso de servidores públicos, contratistas o terceros a las instalaciones de la SIC los fines de semana, debe ser avalado previamente por la Dirección Administrativa a través del coordinador del Grupo de Servicios Administrativos y Recursos Físicos.

- Cualquier ingreso de terceros a las instalaciones de la SIC de lunes a viernes después de las 5:00 p.m., debe ser avalado previamente por la Dirección Administrativa a través del coordinador del Grupo de Servicios Administrativos y Recursos Físicos.

- Sin excepción, todos los visitantes deben llegar al sitio designado para el registro de visitantes (Recepción de las instalaciones) y ser anunciado por el personal de vigilancia al servidor público y/o contratista a visitar.

- El registro de visitantes debe incluir el nombre e identificación del visitante, la fecha y hora de entrada y salida del visitante, y el nombre del servidor público o contratista de la SIC que avala el ingreso.

- La Dirección Administrativa definirá los pisos en los cuales es requerido hacer entrega de un distintivo al visitante, quien deberá entregar en la recepción, un documento de identificación personal vigente diferente a la cédula de ciudadanía, preferiblemente con foto, el cual permanecerá en la recepción durante el tiempo que permanezca dentro de la Entidad.

- Los visitantes deberán ser escoltados por el servidor público o contratista de la SIC, que avala el ingreso durante el tiempo que dure la visita.

- El servidor público y/o contratista de la SIC que avala el ingreso de un visitante, es el encargado de hacerle conocer al mismo sobre los requisitos de seguridad y los procedimientos de emergencia en el área (Ver documento Reglamento de Higiene y Seguridad Industrial y Plan de Emergencias).

- Un visitante no puede avalar el ingreso de otro visitante.

- Las mascotas no son permitidas; sin embargo, algunos animales de asistencia (tales como perros guías) si serán permitidos. En el área del Centro de cómputo no se permitirá ningún animal bajo ninguna circunstancia.

- Los dispositivos electrónicos ingresados por los visitantes tales como portátiles, torres de computador o video beam, deben ser registrados donde se indique la marca del equipo, el modelo y el serial (o su equivalente). Este registro se realizará al ingreso y a la salida de las instalaciones de la SIC.

- Los visitantes que requieran el ingreso a áreas especiales controladas por lectores de tarjetas de acceso, como el centro de datos, pueden solicitar una tarjeta de acceso temporal a través del servidor público que avala su entrada. Las tarjetas temporales se deben devolver una vez finalizada la labor que originó el préstamo de la tarjeta.

6.13.1.1 Distintivos de servidores públicos y contratistas

- El carnet de identificación de los servidores públicos y contratistas es personal e intransferible y de uso obligatorio dentro de las instalaciones de la SIC.

- Todos los servidores públicos y contratistas que se encuentren dentro de las instalaciones de la SIC, están obligados a portar el carnet en forma visible para facilitar su identificación.

- En ningún caso, el servidor público y/o contratista portador del carnet, está facultado a utilizarlo en funciones diferentes o ajenas a la SIC.

- El personal de vigilancia está en la obligación de corroborar la correcta portabilidad del carnet, al momento de ingresar a las oficinas de la SIC.

- En caso de pérdida del carnet, el servidor público y/o contratista debe realizar el denuncio pertinente ante las autoridades competentes y posteriormente reportarlo a la Dirección Administrativa de la SIC.

- Cuando el servidor público y/o contratista se desvincule laboralmente de la SIC, debe entregar el carnet a la Dirección Administrativa.

6.13.1.2 Distintivos de visitantes

- En caso de que se haga entrega de un distintivo a un visitante autorizado, éste debe ser portado visiblemente, durante todo el tiempo que dure la visita. El visitante a su salida deberá entregar el carnet provisto por la SIC al momento de su llegada.

6.13.2 Seguridad perimetral

- Todas las áreas que tienen servicios de procesamiento de información deben ser físicamente seguros (es decir, no deberá haber brechas en el perímetro o áreas donde fácilmente pueda ocurrir una intrusión).

- En los sitios que contengan servicios de procesamiento de información se deben implementar mecanismos robustos físicamente (por ejemplo, cerraduras, barras, alarmas, sistemas lectores de tarjeta, muros, puntos de acceso con vigilancia humana) aplicables para prevenir el acceso no autorizado.

- Las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión.

- Todas las salidas de emergencia de la SIC deben contar con alarma, y deben funcionar de manera segura de acuerdo con el Plan SC04-F30 - Plan de Emergencia.

- Se debe tener un sistema de vigilancia que permita la detección de intrusos.

6.13.3 Seguridad de oficinas, recintos e instalaciones

- Cuando sea posible, las instalaciones de procesamiento de información deberán ser discretas y no tener indicaciones sobre su propósito, sin señales obvias que identifiquen la presencia de actividades de procesamiento de información.

- Los directorios y listados telefónicos internos que indican la ubicación de servicios de procesamiento de información sensible no deben ser de fácil acceso al público.

- Los equipos y dispositivos que son utilizados para soportar las funciones críticas del negocio deben estar en un área de acceso restringido.

- No se debe permitir el uso de equipo de grabación fotográfica, de video o de audio a menos que esté autorizado por el Oficial de Seguridad de la Información.

- Con el propósito de supervisar y registrar las actividades de posibles intrusos, identificar elementos y cualquier tipo de circunstancia que resultase anormal, la SIC, en lo posible, deberá implementar un Circuito Cerrado de Televisión (CCTV), cuya administración estará a cargo de la Dirección Administrativa. Las grabaciones realizadas a través del CCTV, deben ser informadas a todas las personas, incluyendo el propósito, responsabilidades y derechos frente a la misma, de acuerdo con la legislación vigente en materia de protección de datos personales.

- La administración de las grabaciones obtenidas a través del CCTV, será realizada de acuerdo con lo establecido en el documento: GA03–P01. Procedimiento servicios administrativos.

6.13.4 Cámaras fotográficas

Los visitantes no están autorizados para tomar fotografías dentro de las instalaciones de la SIC, a menos que el líder del proceso afectado lo autorice previamente vía correo electrónico.

6.13.5 Protección contra amenazas externas

- El papel y los combustibles deben ser almacenados en lugares aislados en contenedores y en pequeñas cantidades.

- La Dirección Administrativa a través del coordinador del Grupo de Trabajo de Servicios Administrativos y Recursos Físicos, debe instalar en cada área un equipamiento apropiado de seguridad: sistemas de extinción de incendios; salidas de emergencia, cableado, equipamiento de extinción de incendios, etc.

- El uso del cigarrillo es restringido en las áreas internas.

6.13.6 Pólizas de seguros

- El Oficial de Seguridad de la Información, o quien él delegue, y el responsable del activo deben hacer una revisión de las pólizas de seguros asociadas al activo (por ejemplo, hardware) y la cobertura de las mismas desde el momento en que el activo sale de las instalaciones de la SIC.

- Los seguros deben considerar el cubrimiento mínimo de los costos de reposición de los recursos informáticos, costos de interrupción del negocio, el rembolso a

la Entidad por costos en la restauración de las operaciones y pérdidas de ganancias asociadas.

- Se debe considerar específicamente la cobertura en los tiempos de traslado del activo y en las instalaciones donde éste será mantenido.

- En caso de que una o varias pólizas de seguros no tengan cobertura por fuera de las instalaciones de la SIC, se deberá validar la posibilidad de aceptación del riesgo.

6.14 POLÍTICA DE CENTRO DE DATOS

Objetivo:

Establecer los lineamientos para prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de las plataformas tecnológicas para el procesamiento de información de la organización.

6.14.1 Centros de datos en la SIC

- El coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe proveer las condiciones físicas y ambientales para la debida protección y correcta operación de la plataforma tecnológica ubicada en los centros de datos, como sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe supervisar la efectividad de los mecanismos de seguridad física y control de acceso a los centros de datos.

- Las puertas de acceso al centro de datos, deben permanecer siempre cerradas y aseguradas.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

- El acceso a los centros de datos debe ser restringido y solo pueden ingresar personal autorizado por el Jefe de la OTI o a quien él delegue.

- El ingreso de un tercero a un centro de datos debe ser autorizado previamente por el coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien él delegue, y durante su visita debe estar acompañado por un servidor público o contratista de dicho Grupo de Trabajo.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe registrar el ingreso de un tercero a un centro de datos que están bajo su custodia en el formato de ingreso/salida GS01-F05 – Control de acceso al centro de cómputo.

- Los privilegios de acceso físico a los centros de datos de los usuarios autorizados deben ser eliminados a la terminación de la vinculación laboral o contrato laboral, o por alguna novedad.

- Cualquier movimiento dentro de los centros de datos deben ser autorizados por el Oficial de Seguridad de la Información o a quien él delegue, y el Coordinador del Grupo de Trabajo de Servicios Tecnológicos.

6.14.2 Centro de datos externo

- El proveedor debe proporcionar las medidas de seguridad física adecuadas para la prestación de los servicios contratados por la SIC dentro de las instalaciones, como:

    - Las instalaciones deben cumplir con las recomendaciones y directrices de las normas técnicas y estándares internacionales.
    - Sistema de circuito cerrado de televisión
    - Sistema de detección y extinción de incendios

- El proveedor debe proporcionar las medidas de energía adecuadas para la prestación de los servicios contratados por la SIC dentro de las instalaciones, como:

    - Sistemas de UPS configurados en redundancia.
    - Autonomía eléctrica de mínimo 24 horas en caso de interrupción del fluido eléctrico.
    - Alimentación segura a los sistemas de control ambiental

- El proveedor debe proporcionar las medidas ambientales adecuadas para la prestación de los servicios contratados por la SIC dentro de las instalaciones, como contar con un sistema de aire acondicionado.

- El proveedor debe proporcionar las medidas de control de acceso físico a las instalaciones por visitantes y empleados, mediante:

  - Carnet de visitantes
  - Registro de bitácoras
  - Tarjetas de acceso
  - Verificación de autorizaciones previas para el ingreso

- El proveedor debe proporcionar las siguientes medidas de sistema de monitoreo:

  - Operación 7x24 del personal técnico del datacenter.
  - Operación, CAC (Centro de Atención a Clientes) y Monitoreo 7X24.
  - Herramientas de monitoreo para la infraestructura de los diversos fabricantes utilizados.
  - Contar con las herramientas necesarias para detectar y monitorear fallas e interrupciones en los servicios contratados.

- El proveedor debe proporcionar medidas en la gestión en la operación:

  - Debe incluir toda la conectividad para la habilitación del servicio.
  - Debe cifrar las comunicaciones entre la SIC y el Proveedor.
  - El Proveedor debe solicitar aprobación a la SIC, sobre cualquier cambio a realizarse sobre la infraestructura de hardware y software que se haya aprovisionado para la prestación de sus servicios. Las solicitudes de aprobación de cambio deben hacerse con mínimo 48 horas de anticipación.

6.15 POLÍTICA DE EQUIPOS

Objetivo:

Establecer mecanismos para reducir los riesgos de acceso no autorizado, pérdida y daño de información durante y por fuera de las horas laborales normales.

6.15.1 Equipos de usuarios desatendidos

- Todos los computadores y equipos portátiles de la SIC deben tener configurado un protector de pantalla protegido con contraseña, el cual se debe activar después de un período de 5 minutos de inactividad. La reactivación del protector de pantalla debe exigir el ingreso de usuario y contraseña.

- Se deben asegurar los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente, por ejemplo, acceso con contraseña, cuando no están en uso.

- Se debe cerrar (Log-Off) las aplicaciones o servicios de red cuando ya no se necesiten.

- Los equipos de cómputo deben localizarse preferiblemente en ubicaciones físicas de modo que las pantallas no queden expuestas y puedan ser visualizadas por personas externas.

6.15.2 Escritorio limpio y pantalla limpia

- Cada vez que un servidor público o contratista de la SIC se ausente de forma temporal o definitiva de su puesto de trabajo, debe bloquear la pantalla del computador a su cargo.

- Cada vez que un servidor público o contratista se ausente de forma temporal o definitiva de su puesto de trabajo, no debe haber información sensible o crítica de la SIC sobre el escritorio, por ejemplo, documentos físicos o medios de almacenamiento electrónico, por lo que se deben guardar (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requieran.

- Se debe evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales).

- Los documentos que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente y debe ser destruida.
- No se debe reutilizar documentos impresos con información clasificada o sensible ni utilizarlos como papel reciclable.

- No se debe consumir alimentos y/o bebidas cerca de los elementos de cómputo.

- Todo servidor público, contratista o tercero debe evitar el uso de iconos y accesos innecesarios en el escritorio digital del computador.

6.16 POLÍTICA DE RETIRO DE ACTIVOS DE INFORMACIÓN FÍSICOS

Objetivo:

Asegurar la implementación de controles para la seguridad de equipos y activos fuera de las instalaciones.

- Ningún activo de información físico o digital (equipos, información, software) se debe retirar de las instalaciones de la SIC sin autorización del responsable del activo.

- La solicitud del retiro del activo debe ser realizada por los líderes del proceso y autorizada por el Director Administrativo mediante el formato GA03-F05 - Ingreso o retiro de bienes.

- Los servidores públicos de la SIC, contratistas o terceras partes con autoridad para permitir el retiro de activos de información deben estar claramente identificados.

- Se debe registrar el retiro y la devolución de un activo de información físico, verificando los tiempos acordados para el retiro.

- El responsable del activo debe evaluar los riesgos asociados al proceso de retiro, transporte y ubicación del activo en el sitio de destino durante el tiempo que duré fuera de las instalaciones de la SIC.

6.16.1 Seguridad de equipos fuera de las instalaciones

- Cuando se envíen equipos de cómputo a diferentes ciudades, se debe contar con un embalaje en el traslado de equipos de cómputo, para proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito.

- Los equipos y medios que se encuentran fuera de las instalaciones de la SIC no se deben dejar solos en sitios públicos. Los equipos portátiles se deben llevar como equipaje de mano.

- Se deben seguir las recomendaciones del fabricante de los equipos respecto a la protección de los mismos frente a factores externos, como temperatura, campos electromagnéticos, humedad, etc.

- Se debe tener claridad sobre la cobertura de pólizas de seguro de los equipos por fuera de las instalaciones.

- Se deben aplicar controles apropiados para los riesgos identificados en aquellos sitios donde se realicen labores con los equipos por fuera de las instalaciones de la SIC, ya que son de uso exclusivo para actividades de la Entidad (por ejemplo, el lugar de residencia o domicilio del usuario u otras organizaciones en las cuales se realicen actividades laborales).

- En caso de portátiles, se recomienda cifrar el disco duro y configurar el acceso al sistema operativo con un ID de usuario y una contraseña que cumpla con la política de contraseñas (ver numeral 6.10 Política de Contraseñas en este documento).

6.17 POLÍTICA DE RETIRO DE ACTIVOS DE INFORMACIÓN DOCUMENTALES

Objetivo:

Dar los lineamientos para la protección de medios que contienen información durante el transporte.

- El coordinador del Grupo de Trabajo de Gestión Documental y Archivo, es el responsable del préstamo interno de expedientes de gestión a usuarios internos. El usuario realizará la solicitud por medio del Sistema de Trámites en el módulo de Administración de Expedientes, según se dispone en el documento GD01-P01 - Procedimiento Archivo y Retención Documental.

- El coordinador del Grupo de Trabajo de Gestión Documental y Archivo, es el responsable del préstamo de expedientes de gestión a usuarios externos. La consulta se podrá realizar únicamente en sala por el solicitante, según se dispone en el documento GD01-P01 - Procedimiento Archivo y Retención Documental.

- Cuando un servidor público requiera trasladar un documento a otra dependencia en calidad de préstamo, la dependencia productora debe llevar un registro en el que se consigne la fecha de préstamo, identificación del expediente y/o carpeta, número de folios, datos del solicitante, registro de devolución y término para su devolución, de acuerdo al formato GD01-F07 – Control préstamo interno de documentos.

- Toda solicitud de documentos y/o fotocopias que se requieran del Archivo Central (historias laborales, resoluciones, consecutivos, contratos, etc.) se debe solicitar mediante el Sistema de Gestión de Archivo en el Módulo de Préstamo, según se dispone en el documento GD01-P01 - Procedimiento de Archivo y Retención Documental.

- Con el fin de garantizar y dar cumplimiento a los horarios establecidos para la entrega y préstamo de expedientes a los usuarios internos y externos, se requiere establecer horarios de transporte (suministrado por la Dirección Administrativa), para el adecuado control, búsqueda y traslado de expedientes desde la sede del Archivo Satélite hasta la sede Centro de la SIC y viceversa, según se dispone en el documento GD01-P01 – Procedimiento de Archivo y Retención Documental.

- La remisión de los documentos de los archivos de gestión y de los satélites al Archivo Central, debe realizarse con la periodicidad que se establezca en la tabla de retención documental para cada una de las series, definidas por la SIC.

- En la transferencia de documentos deben considerarse todas las medidas que garanticen la conservación del material, tales como la manipulación, embalaje y transporte, entre otras, y aquellas que eviten la contaminación y propagación de factores nocivos.

6.18 POLÍTICA DE CONTROL DE CAMBIOS

Objetivo:

Controlar que los cambios aplicados a activos de información (Hardware y Software) de la Oficina de Tecnología e Informática de la Superintendencia de Industria y Comercio, pasan por un proceso de revisión, pruebas y aprobación que compruebe que el cambio no generará impacto sobre el entorno operativo ni la infraestructura tecnológica.

- El jefe de la OTI debe establecer un comité asesor de cambios (CAB) y un comité asesor de cambios de emergencias (ECAB), quienes asuman el rol deben contar con las competencias y habilidades requeridas y definidas para la toma de decisiones; de cada reunión que se realice se debe generar un acta con los cambios aprobados y rechazados.

- Solo serán planificados e implementados los cambios sobre los servicios pactados, que hayan sido autorizados por el CAB o ECAB de acuerdo con su impacto y urgencia.

- Cualquier tipo de cambio en la plataforma tecnológica debe estar formalmente documentado y aprobado desde su solicitud hasta su implantación, excepto si se trata de una situación de emergencia, esto para mantener un rastro para auditoría de todos los cambios realizados (Ver el documento Procedimiento control de cambios). En situaciones de emergencias se deberá registrar el cambio realizado y su justificación.

- La implementación de los cambios se debe realizar en el momento oportuno para no perturbar los procesos de negocios involucrados.

6.19 POLÍTICA DE CONTROL DE CÓDIGO MALICIOSO

Objetivo:

Proporcionar los lineamientos para implementar controles de detección, prevención y recuperación, para la protección de la integridad de la información y de la plataforma tecnológica de la Superintendencia de Industria y Comercio frente a códigos maliciosos.

- Toda la infraestructura tecnológica y de procesamiento de información, y de comunicaciones, deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe disponer de herramientas de detección de códigos maliciosos tales como antivirus, antimalware, antispam, antispyware, entre otras, las cuales siempre debe estar actualizado con las últimas definiciones del fabricante del software.

- El software de detección de códigos maliciosos debe estar configurado para realizar las siguientes acciones:

  - Verificar la presencia de códigos maliciosos en archivos de medios ópticos (CDs, DVDs), electrónicos (discos duros) y aquellos obtenidos por medio de una red antes de su uso.
  - Verificar la presencia de códigos maliciosos en los archivos adjuntos y las descargas del correo electrónico antes de su uso.
  - Verificar los códigos de las páginas web para comprobar la presencia de códigos maliciosos.
  - Verificar la presencia de códigos maliciosos en los archivos que se dispongan a ser enviados a un servidor (correo, archivos compartidos) u otro equipo de la red.

- El Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, es responsable de la instalación, actualización y el aseguramiento de uso constante del software de detección de códigos maliciosos (especialmente en los computadores personales y los servidores de archivo de la red).

- El Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe asegurar que, a las herramientas de software de detección de códigos maliciosos no se les pueda realizar cambios en la configuración ni ser deshabilitadas de los equipos, y deban ser actualizados permanentemente.

- El jefe de la OTI a través de la coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, deberá proporcionar mecanismos para la concienciación referente a la protección y prevención contra el software malicioso, a todos los usuarios de la SIC. De forma periódica se debe dar a conocer a los usuarios sobre nuevos tipos de códigos maliciosos a los cuales pueden ser vulnerables.
- En caso de sospecha de infección de código malicioso, se debe seguir el procedimiento de Gestión de Incidentes. (Ver el documento SC05-P01 - Procedimiento de gestión de incidentes).

- Es responsabilidad de los usuarios reportar todos los incidentes de infección de virus a la mesa de servicios, para que a través de la OTI se tomen las medidas de contención de conformidad con el documento SC05-P01 Procedimiento de gestión de incidentes.

- Todos los sistemas operativos y aplicativos deben tener instalados los parches y las últimas actualizaciones de seguridad aplicables para bloquear todas las vulnerabilidades de seguridad conocidas.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, será el encargado de revisar y recibir las actualizaciones de seguridad o notificaciones de aplicación de parches de seguridad. (Ver el documento Procedimiento de instalación de parches de seguridad).

- Todo programa de código fuente de los sistemas de información y desarrollos de software de la SIC, se debe examinar antes de utilizar los programas en producción.

6.20 POLÍTICA DE BACKUPS

Objetivo:

Establecer los lineamientos para mitigar el riesgo de pérdida de la información definiendo la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información, software y sistemas.

6.20.1 Backup de Sistemas de Información

- El Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, es el responsable de realizar las copias de respaldo de la información.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá documentar un plan de backups de la SIC, previamente diseñado en conjunto con los propietarios de los sistemas de información y los recursos tecnológicos, donde se establezca el tipo de backup, a qué se le realiza el backup, cuándo se realiza, con qué periodicidad y cuál es la criticidad para realizar las copias de respaldo de información.

- Se deben registrar en el formato GS01-F11 - Formato de registro de backup de la Información, todas las copias de respaldo que se realicen indicando el tipo de backup, la periodicidad, la fecha de creación y el periodo de retención. La actividad de generación de las copias de respaldo debe realizarse de acuerdo con el formato GS01-F12 - Formato definición de backup de la Información.

- Todos los backups deben ser retenidos de acuerdo con lo establecido en el formato GS01-F12 - Formato definición de backup de la Información.

- La generación de copias de respaldo se debe realizar con base en el resultado de los análisis de riesgos de la información existente y vigente en la SIC.

- En el caso de sistemas y servicios críticos, las disposiciones relativas a copias de respaldo, deberán abarcar toda la información de sistemas, aplicaciones y datos necesarios para recuperar el sistema completo en caso de desastre.

- La mesa de servicios debe validar que los backups fueron ejecutados exitosamente para cada activo de información definido en el documento GS01-F12 - Formato de definición de backups de la Información. En el caso de que se encuentre una falla en la ejecución o en el resultado del backup, se debe iniciar manualmente el backup para dicho activo y se debe informar de la incidencia de acuerdo a la Política de Gestión de Incidentes.

- El almacenamiento de las copias de respaldo es responsabilidad de la OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces.

- Los respaldos se deben almacenar en un sitio seguro remoto que otorgue protección física y ambiental que permita mantener su integridad y disponibilidad, dado un desastre o una amenaza ambiental.

- Los medios de respaldo se deben probar con regularidad para garantizar que sean confiables en situaciones de emergencia. La responsabilidad de la verificación es de la OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces. En caso de que el proceso de restauración haya generado errores y no termine exitosamente, el Coordinador del Grupo de Trabajo de Servicios Tecnológicos, o quien él delegue, deberá informar del incidente de acuerdo a la política de gestión de incidentes. (Ver numeral 6.29 - Política de gestión de incidentes en este documento).

- Los administradores de los aplicativos y sistemas de información, y los usuarios finales, no deben almacenar información sobre las particiones que han sido destinadas y asignadas como repositorio del sistema operativo o de los aplicativos.
- Las copias de respaldo generadas se pueden almacenar en medios estándares como cintas, discos duros externos o medios ópticos (CD, DVD, Blu Ray), sin embargo, se deben escoger medios que no tengan un tiempo de deterioro menor a seis (6) meses según las especificaciones del fabricante. En donde aplique, se establecerá un estándar de archivo de compresión.

- Después de vencido el periodo de retención se debe eliminar el contenido los medios estándares de almacenamiento utilizados de acuerdo con las políticas y procedimientos aplicables (ver numeral 6.8 - Política de gestión de medios removibles en este documento).

- El acceso al registro de ubicación y contenido de los medios debe estar restringido y será autorizado únicamente al Grupo de Trabajo de Servicios Tecnológicos, o al personal que sea aprobado por el Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue.

- Los respaldos deben estar adecuadamente configurados de tal forma que sean fácilmente identificables

- Cada treinta (30) días, la mesa de servicios realizará una recuperación o restauración aleatoria de datos para verificar la consistencia e integridad de los mismos y de esta manera, tener la certeza que, en caso de presentarse algún tipo de contingencia, las copias de seguridad sean una alternativa confiable de recuperación de la información. Estas pruebas de restauración se realizarán sobre ambientes de pruebas controlados con el fin de validar la efectividad de los respaldos.

- En cuanto a solicitudes por demanda, los líderes de proceso y jefes son los únicos autorizados para solicitar el respaldo y/o restauración de información indicando los datos del solicitante, datos de la aplicación, datos de los archivos (tipo y ubicación), datos de la BD (ubicación, motor y versión), accesos, periodicidad del respaldo y tipo de respaldo. Estas solicitudes deben realizarse a través de la herramienta de gestión de servicios de TI.

6.20.2 Backup de usuarios finales

Para los backups de usuario final se debe tener en cuenta las siguientes situaciones:

a) Cuando el contratista o servidor público se encuentra en ejercicio de sus funciones u obligaciones contractuales:

- Es responsabilidad de los usuarios entregar una copia de la información generada en función de sus labores, al finalizar la vinculación laboral con la SIC.

b) Cuando se presenta una terminación de la vinculación laboral o cambio de responsabilidades del contratista o servidor público.

- Los contratistas o servidores públicos deben gestionar la entrega de la información a la Oficina de Tecnología e Informática, solicitando a la mesa de servicios de la SIC la respectiva toma del backup. Una vez surtida esta actividad

pueden proceder a solicitar la firma del paz y salvo que soporta la correcta ejecución de la misma.

6.21 REGISTRO (LOGING) Y SEGUIMIENTO

Objetivo:

Definir el registro de eventos y la realización de monitoreo sobre los registros.

6.21.1 Registro de eventos

- La Coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe generar registros de auditoría de eventos relacionados con la seguridad de la información.

- La Coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá comunicar las fallas en el procesamiento de la información que permita tomar medidas correctivas.

- La Coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe monitorear y revisar periódicamente los registros de auditoría de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

- Todos los eventos de seguridad relevantes de un servidor que alberga información confidencial deben ser registrados en un log de eventos de seguridad. Esto incluye errores en autenticación, modificaciones de datos, utilización de usuarios privilegiados, cambios en la configuración de acceso a archivos, modificación a los programas o sistema operativo instalados, cambios en los privilegios o permisos de los usuarios o el uso de cualquier función privilegiada del sistema.

- El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones. Estos registros deben incluir lo siguiente:

  - Nombre de la persona que reporta la falla.
  - Hora y fecha de ocurrencia de la falla.
  - Descripción del error o problema.
  - Responsable de solucionar el problema.
  - Descripción de la respuesta inicial ante el problema.
  - Descripción de la solución al problema.
  - Hora y fecha en la que se solucionó el problema.

Los registros de fallas deben ser revisados semanalmente. Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una solución al problema. Además, estos registros deben ser almacenados para una posterior verificación independiente.

- La Coordinación del Grupo de Trabajo de Sistemas de Información o quien haga sus veces, debe generar a la Dirección Financiera trimestralmente o por solicitud, de acuerdo con sus necesidades, los registros de auditoría de posibles cambios no autorizados en la base de datos de cartera por multas.

6.21.2 Protección de la información de registro

- La Coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe salvaguardar los registros de auditoría que se generen en la plataforma tecnológica y los sistemas de información, para certificar la integridad y disponibilidad de los mismos.

- Los registros solo deben ser accedidos por personal autorizado.

- Los “logs” (bitácoras) de seguridad deben ser almacenados por un periodo mínimo de tres (3) meses. El acceso a dichos logs debe ser permitido solo a personal autorizado por el coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien haga sus veces. En la medida de lo posible, los logs deben ser almacenados en medios de “solo lectura”.

6.21.3 Registros (logs) del administrador y del operador

- Las actividades del administrador y del operador del sistema se deben registrar.

- Los administradores de sistemas no deben tener permiso para borrar o desactivar registros (logs) de sus propias actividades.

6.21.4 Sincronización de relojes

- La OTI a través de quien delegue el coordinador del Grupo de Trabajo de Servicios Tecnológicos, debe sincronizar los relojes de todos los sistemas con una única fuente de referencia de tiempo como la hora legal colombiana (http://horalegal.inm.gov.co/), para asegurar la exactitud de todos los registros de auditoría, que pueden ser necesarios para investigaciones o como evidencia legal en casos legales o casos disciplinarios.

6.22 POLÍTICA DE INSPECCIÓN DE SISTEMAS DE INFORMACIÓN

Objetivo:

Inspeccionar periódicamente los Sistemas de Información de la SIC.

- La coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, deberá planificar periódicamente inspecciones de los sistemas de información en producción.

- La coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, debe definir el alcance de las pruebas técnicas de inspección.

- Las pruebas de inspección que puedan afectar la disponibilidad del sistema se deberán realizar fuera de horas laborales.

- Las pruebas de inspección se deberán limitar a acceso a software y datos únicamente para lectura.

- El acceso diferente al de solo lectura solamente se deberá prever para copias aisladas de los archivos del sistema (system files), que se deberán borrar una vez que la inspección haya finalizado, o se deberá proporcionar protección apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría.

- La mesa de servicios es responsable de la inspección y monitoreo frecuente de los logs y de los registros de control de los aplicativos en funcionamiento. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría; por tal razón, deben protegerse para conservar su integridad y confidencialidad.

- La coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, deberá documentar mediante un informe, los resultados de las inspecciones de los sistemas de Información de la SIC y presentarlos a la jefatura de la OTI.

6.23 POLÍTICA DE LA GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

Objetivo:

Dar lineamientos para evaluar la exposición de la Superintendencia de Industria y Comercio a las vulnerabilidades técnicas de información.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, se encargará de identificar las vulnerabilidades técnicas de las plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, ejecutará un escaneo de vulnerabilidades técnicas en las plataformas tecnológicas tres (3) veces al año. Se debe documentar e informar a la mesa de servicios y a la jefatura de la OTI los hallazgos de las vulnerabilidades técnicas, y las acciones apropiadas y oportunas realizadas para minimizar el nivel de riesgo.

- Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura de los riesgos identificados asociados a las vulnerabilidades técnicas.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, realizará seguimiento y verificación de que se hayan corregido las vulnerabilidades técnicas.

- Toda acción tomada para el tratamiento de una vulnerabilidad técnica en el ambiente productivo, deberá surtir el procedimiento de gestión de cambio tecnológico.

- Los colaboradores de la SIC que utilizan los servicios y sistemas de información de la Entidad, al momento de observar cualquier debilidad de seguridad de la información, están obligados a reportarlo por los canales establecidos y no deben ser aprovechados de manera maliciosa.

6.24 POLÍTICA GESTIÓN DE SEGURIDAD EN LAS REDES

Objetivo:

Establecer mecanismos de control para la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

6.24.1 Controles de redes

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces junto con la mesa de servicios, debe establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe establecer las responsabilidades y procedimientos para la gestión de equipos de redes.

- Los usuarios de la red interna de la SIC, no pueden realizar o ejecutar acciones en la red que sean exclusivas de los administradores de red.

- Los servidores públicos y contratistas no deben llevar a cabo ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, equipos tecnológicos para interconexión de equipos en la red, ni cambiar su configuración sin haber sido formalmente aprobados por la OTI.

- Es responsabilidad del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, determinar lo siguiente:

  - Elementos de la red que pueden ser accedidos.
  - El procedimiento de autorización para la obtención de acceso.
  - Controles para la protección de la red.

- Todos los servicios habilitados en los sistemas deben contar con una justificación coherente con las necesidades de la Entidad. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio.

6.24.2 Seguridad de los servicios de red

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la SIC.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe instalar protección entre las redes internas de la SIC y cualquier red externa con el objetivo de proteger la información de la SIC de amenazas externas, para lo cual puede utilizar dispositivos de seguridad perimetral tales como firewalls, sistema de detección de intrusos, entre otros.

- Se debe asegurar de que los proveedores de servicio de redes implementen mecanismos de seguridad.

6.24.3 Separación en las redes

- La SIC debe considerar la separación de redes que requieran distintos niveles de seguridad y tráfico. Esta separación debe realizarse de acuerdo con la clase de información albergada en los sistemas que constituyen dichas redes. Esto debe incluir equipos de acceso público.

- La SIC debe separar las redes y los grupos de servicios de información dividiéndolas en dominios lógicos de red, cada uno protegido por un perímetro de seguridad definido.

- Cada dominio creado debe ser aprobado por el Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue, y debe ser actualizado en el mapa de red de datos de la Entidad.

- Las redes inalámbricas deben estar separadas de la red principal de usuarios con el fin de minimizar el riesgo en los activos de información. El acceso a estas redes inalámbricas debe ser controlado, debe tener una autenticación segura en los casos que se requiera.

6.24.4 Conexión remota por medio de Red Privada Virtual (VPN)

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe garantizar que la conexión remota a la red interna de la SIC, debe realizarse a través de una conexión VPN SSL, suministrada por la Entidad.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe establecer métodos apropiados de autenticación, para los usuarios que utilicen accesos remotos.

- Toda solicitud de creación de VPN, debe ser realizada en los formatos publicados en el SIGI, los cuales deben ser aprobados por el jefe inmediato (que tenga como mínimo cargo de coordinador del grupo de trabajo) del funcionario o por el supervisor del contrato en el caso de los contratistas.

- Al establecer conexiones VPN haciendo uso de equipos ajenos a la Entidad, los usuarios entienden y aceptan que sus equipos de cómputo son una extensión de la red de datos de la SIC, y por esta razón deben cumplir con las mismas políticas que aplican para los equipos propiedad de la SIC.

- Es responsabilidad de los usuarios que utilizan los servicios de VPN, asegurar que personas no autorizadas accedan a las redes de datos internas de la SIC.

Si la VPN no se ha utilizado en al menos los últimos 90 días, ésta será eliminada. Pasado ese tiempo, en caso de requerirse nuevamente, debe surtir de nuevo todo el proceso para la creación, incluyendo el diligenciamiento del formato respectivo.

6.25 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Objetivo:

Mantener la seguridad de la información transferida dentro de una organización y con cualquier Entidad externa.

6.25.1 Transferencia de información

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá implementar controles para proteger la información transferida a otras Entidades contra interceptación, copiado, modificación, y destrucción.

- Los colaboradores de la SIC no debe emitir copias, divulgar, emplear indebidamente, o reproducir por cualquier medio, datos o información contenida en los aplicativos, bases de datos y sistemas de información a los cuales se le haya otorgado acceso, con fines diferentes al cumplimiento de sus funciones o labores contratadas.

- La OTI a través del Grupo de Servicios Tecnológicos o quien haga sus veces, deberá implementar mecanismos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.

- La información digital que sea transferida por Entidades externas a la SIC, deben ser revisados previamente por su emisor con el fin de detectar posible malware o código malicioso.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá establecer un control especial tal como criptografía, para proteger la confidencialidad, la integridad y la autenticidad de la información.

- El personal no debe tener conversaciones confidenciales en lugares públicos, o mediante canales de comunicación no seguros, oficinas abiertas y lugares de reunión, entre otros.

- Es responsabilidad del personal, las partes externas y cualquier otro usuario no comprometer a la Entidad, por ejemplo, por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.

6.25.2 Acuerdos sobre transferencia de información

- Las dependencias que requieran realizar trasferencias externas de información, deberán establecer los lineamientos para proteger, controlar y notificar la transmisión, despacho y recibo de la información, así mismo deberá establecer cláusulas de confidencialidad entre la SIC y las partes externas, para lo cual pueden apoyarse del Oficial de Seguridad de la Información.

- Los datos e información creados, almacenados y recibidos, serán propiedad de la SIC, en este sentido, para transferir cualquier tipo de información clasificada o reservada se debe contar con autorización escrita del jefe inmediato.

- Copia, sustracción, eliminación, modificación, daño intencional o utilización de la información para fines distintos a las labores institucionales, serán sancionadas de acuerdo con las normas y legislación vigentes, inclusive cuando se haya dado con posterioridad a la finalización del contrato.

6.25.3 Acuerdos de confidencialidad y no divulgación

- La SIC a través del coordinador del Grupo de Trabajo del Talento Humano y el coordinador del Grupo de Contratación deberán establecer los acuerdos de confidencialidad y no divulgación para ser incorporados como parte integral de los contratos laborales para proteger la información de la Entidad, e informar a los firmantes acerca de su responsabilidad y acciones para evitar divulgar información no autorizada.

- Los acuerdos de confidencialidad y no divulgación de información son aplicables a todos los servidores públicos y contratistas quienes deberán aceptar y firmar los acuerdos de la Entidad.

- Los acuerdos de confidencialidad y de no divulgación deben cumplir todas las leyes y reglamentaciones aplicables para la jurisdicción pertinente.

Los requisitos para los acuerdos de confidencialidad y de no divulgación se deben revisar periódicamente, y cuando ocurran cambios que influyan en éstos.

6.26 POLÍTICA PARA ENTORNOS DE DESARROLLO, PRUEBAS Y PRODUCCIÓN

Objetivo:

Reducir los riesgos de acceso o cambios no autorizados en sistemas de información y proteger la información sensible utilizada en entornos de prueba, desarrollo y producción de la Oficina de Tecnología e Informática de la Superintendencia de Industria y Comercio.

6.26.1 Separación de recursos

- La OTI, deberá separar los ambientes de desarrollo, prueba y producción, de manera física y lógica. Para cada ambiente se define el siguiente alcance:

  ✓ Ambiente de desarrollo: Será utilizado para crear nuevas aplicaciones, desarrollar nuevas características a las aplicaciones existentes o corregir errores.

  ✓ Ambiente de pruebas: Este entorno es utilizado para probar aplicaciones e informar sobre los errores o las características faltantes de las aplicaciones, las cuales deben ser ajustadas antes de la publicación final.

  ✓ Ambiente de producción: En este entorno se ejecuta las aplicaciones que utilizan los usuarios finales. Las modificaciones previstas sobre este ambiente, deben surtir el procedimiento de gestión del cambio tecnológico.

- La separación de ambientes de desarrollo, prueba y producción, de los diferentes aplicativos y sistemas de información de la SIC, se realizará teniendo en cuenta los recursos de la infraestructura tecnológica disponible.
- La OTI a través de los Grupos de Trabajo de Sistemas de Información y Grupo de Trabajo de Gestión Información y Proyectos Informáticos, deberá definir establecer lineamientos para la transferencia de información de un entorno de prueba a un entorno de producción.

- El software de desarrollo y el software de producción se debe ejecutar en diferentes plataformas computacionales y en diferentes dominios o directorios.

- Compiladores de código, editores u otras herramientas de desarrollo no deben ser accesibles en un sistema operativo cuando no se requiera.

- Los entornos de prueba deben emular estrechamente a los entornos de producción.

- Los desarrolladores no deben tener acceso al entorno de producción.

- Las aplicaciones en ambiente de desarrollo y de pruebas no deben estar expuestas en internet.

- Los entornos de prueba y producción deben tener mensajes de identificación apropiados que permitan al usuario reconocer el tipo de entorno en el que se encuentra y reducir el riesgo de un error.

- Un entorno de prueba no debe contener copias fieles de los datos en producción.

- Los entornos de desarrollo y pruebas deben tener un mecanismo de monitoreo y control de cambios que permitan hacer seguimiento a los desarrollos y los responsables de los mismos y permitan identificar códigos maliciosos introducidos.

- Por medio del control de cambios se debe asegurar que todos los cambios del modelo y ambientes de producción hayan sido revisados y aprobados por el (los) jefes(s) de dependencia(s) correspondientes.

6.26.2 Protección de datos de prueba

- Los entornos de prueba deben contar con un mecanismo de control de acceso similar al utilizado en entornos de producción.

- Se deben registrar las acciones de copia y utilización de información de un entorno de producción.
- Se debe evitar el uso de información de entornos de pruebas que contengan información personal u otro tipo de información sensible.
- Si se usa información personal o sensible en un entorno de pruebas, los detalles y el contenido sensible se deben retirar o modificar antes de su uso.

6.26.3 Política de desarrollo seguro

- La SIC debe definir y aplicar principios y lineamientos de seguridad para la metodología de desarrollo de software que utilice, incluyendo aspectos como requisitos de seguridad, análisis de vulnerabilidades, revisión de código, pruebas de carga, protección de datos de prueba, y en general requisitos de seguridad en los sistemas de información. Estos principios y lineamientos de seguridad deben ser documentados y tratados como aspectos de la arquitectura de TI de la SIC.

6.26.4 Creación y eliminación de sistemas de información

- Los proyectos que involucren el desarrollo de nuevos sistemas de información deben responder a necesidades de la entidad revisadas y aprobadas por la Oficina de Tecnología e Informática y deben encontrarse debidamente incorporadas en la planeación institucional o aprobadas como estrategias internas o de mantenimiento de la OTI.

- La Oficina de Tecnología e informática debe realizar la identificación de requisitos de seguridad de la información para los nuevos sistemas de información o nuevos módulos de los sistemas existentes durante la etapa de identificación de requerimientos funcionales. Adicionalmente todo nuevo desarrollo de sistema de información deberá dar cumplimiento a los principios y lineamientos de seguridad definidos para la metodología de desarrollo de software adoptada por la OTI. El Grupo de Trabajo de Informática Forense y Seguridad Digital será el encargado de facilitar y verificar el cumplimiento de estos principios y lineamientos.

- La eliminación de cualquier sistema de información debe ser aprobado por el comité de cambios de la OTI y entre sus actividades debe incluir, los requisitos del área responsable del sistema de información, requisitos de retención documental, actividades de backup final y eliminación segura de datos y usuarios.

6.26.5 Acceso con privilegios de usuario administrador a los sistemas de información.

- La OTI a través de las coordinaciones de sus grupos de trabajo o quién ellos deleguen, tiene la autoridad para designar a un usuario como administrador de un sistema de información, en consecuencia, deben brindar la transferencia de conocimiento necesaria para que el usuario administrador autorizado haga uso seguro y eficiente de los privilegios otorgados.

- La OTI a través de las diferentes coordinaciones de sus grupos de trabajo o quién ellos deleguen, en conjunto con las dependencias funcionales, deben verificar semestralmente que los niveles de acceso (o también llamados niveles de privilegios) asignados a los usuarios sean apropiados de acuerdo con el propósito de la SIC y se conserve la separación de funciones, definiendo además si los permisos otorgados siguen vigentes o se deben ajustar o eliminar. Lo anterior sin perjuicio de las actualizaciones a realizar durante el ejercicio periódico de la gestión de usuarios y privilegios.

6.27 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Objetivo:

La Superintendencia de Industria y Comercio – SIC en procura de mantener la seguridad y privacidad de la información que se encuentra en los activos de información y los cuales son accedidos, procesados, modificados, almacenados, transferidos y/o eliminados por los proveedores (tercero, aliados estratégicos), se establece que se deberá contar con mecanismos y controles de seguridad definidos de acuerdo con el nivel de clasificación de los activos de información; garantizando que éstos se encuentren adecuados y alineados a lo establecido en el Modelo de Seguridad y Privacidad de la Información - MSPI.

El objetivo es definir los lineamientos para asegurar la protección de los activos de la organización que sean accesibles a los proveedores. Estos lineamientos deben ser conocidos y aplicados por los proveedores y/o terceros que prestan servicios a la Entidad.
Cuando la SIC suscriba un contrato con diferentes proveedores, se deberá tener en cuenta las siguientes consideraciones:

- Identificar los tipos de proveedores que actualmente tiene la Entidad para su debido seguimiento y auditoría sobre el cumplimiento de los controles de seguridad.

- Definir el tipo de acceso que tendrá el proveedor a la información; Dependiendo del tipo de acceso y activos entregados, generados, procesados, consultados, transmitidos; el proveedor deberá garantizar el cumplimiento de los controles de seguridad definidos en el MSPI.

- El proveedor deberá determinar el procedimiento para la gestión de eventos, incidentes, contingencia y recuperación de la información asignada, alineados a los controles de seguridad de la Entidad.

- Asegurar la formación y entrenamiento realizado por el proveedor respecto a la concienciación sobre el manejo de la información de acuerdo con las políticas, guías y/o procedimientos de la Entidad.

- Asegurar la definición de las responsabilidades de cada parte para acordar e implementar controles de acceso, revisión, seguimiento, reporte y auditoría.

- Asegurar el procedimiento de devolución de activos físicos y/o lógicos, generados, modificados, y/o que tengan almacenados en sistemas de información diferentes a los autorizados por la entidad.

- Asegurar el cumplimiento de los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual, derechos de autor, y una descripción de cómo se asegurará su cumplimiento.

- La Entidad debe llevar a cabo la evaluación respectiva de riesgos de seguridad y privacidad de la información asociada tanto a la información entregada, generada procesada, consultada, transmitida, eliminada, por los proveedores (terceros, aliados estratégicos).

- El (los) supervisor (es) del contrato en conjunto con el Oficial de Seguridad de la Información – CISO serán los encargados de revisar que se incluyan los acuerdos de confidencialidad y cumplimiento de políticas de seguridad de la Entidad en los contratos y/o acuerdos con los proveedores.

- El (los) supervisor (es) del contrato en conjunto con el Oficial de Seguridad de la Información - CISO propenderán que la información a la cual tienen acceso los aliados estratégicos mantenga su clasificación designada: Pública Clasificada, Pública Reservada y/o Pública.

- Se debe garantizar procesos de auditabilidad sobre el cumplimiento de acceso lógico y físico a nivel de los activos de información a los cuales se les ha brindado el permiso a los proveedores (terceros, aliados estratégicos) para consulta, modificación, uso, eliminación y generación de información.

- La entidad definirá los requisitos de seguridad en los procesos de adquisición de productos y/o servicios de tecnología de la información y comunicaciones para la SIC; garantizando que los nuevos productos y servicios cumplen con los requisitos de seguridad establecidos en su línea base.
- La SIC deberá gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

Para garantizar el cumplimiento de los lineamientos de seguridad por parte de los proveedores y/o terceros, la SIC y/o quien designe realizará las siguientes actividades:

- Validación de los informes de servicios elaborados por los proveedores y/o terceros.

- Realización de auditorías de cumplimiento de controles de seguridad.

- Realizará seguimiento a los incidentes de seguridad de la información que presente el proveedor en los informes periódicos acordados.

- Validar los niveles de continuidad del servicio acordados con el proveedor.

- Validar los cambios que deban realizar los proveedores sobre las aplicaciones gestionadas a través del proceso de cambios definido por la Entidad y el proveedor.

6.28 POLÍTICA DE BORRADO SEGURO

Objetivo:

Prevenir el robo de la información de los activos de información que se dan de baja o van a ser utilizados por otro servidor público en la Superintendencia de Industria y Comercio.

- El Grupo de Trabajo de Servicios Tecnológicos y Seguridad Digital, o quien haga sus veces, junto con el Almacén debe asegurar el borrado seguro de información digital de los equipos de cómputo retirados, el cual debe promover el uso de métodos que sobrescriban al menos tres veces el medio de almacenamiento.

- El borrado seguro de información digital debe efectuarse, entre otros casos, cuando se libera y retorna al almacén un equipo de cómputo, portátil o dispositivo de almacenamiento extraíble de propiedad de la Entidad, para ser reasignado o darse de baja, de igual forma, si fueron alquilados y serán retornados al proveedor o en el evento de finalización del periodo de retención de archivos digitales de acuerdo con las tablas de retención documental.
- Para aplicar el borrado seguro de información utilizando el método de destrucción física, aplicable al papel y dispositivos no regrabables, los servidores públicos, contratistas y terceros de la Entidad pueden utilizar las trituradoras dispuestas en la Entidad. No obstante, antes de aplicar este método se debe tener en cuenta las tablas de retención documental de la SIC.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe realizar el borrado remoto de información en los dispositivos móviles institucionales en caso de pérdida o hurto, con el fin de eliminar los datos

de dichos dispositivos y restaurarlos a los valores de fábrica, evitando así divulgación no autorizada de información.

6.29 POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Asegurar un enfoque consistente, rápido, efectivo y ordenado para la gestión de los incidentes de seguridad de la información en la Superintendencia de Industria y Comercio.

- Todos los servidores públicos, contratistas y terceros directos o indirectos deben reportar a través de la mesa de servicios, cualquier situación sospechosa, incidente o punto débil que exista en los sistemas o servicios y que comprometa la confidencialidad, integridad y disponibilidad de la información; de no hacerlo, se considerará cómplice de dicho incidente y tendrá que responder, dependiendo de la gravedad del incidente, ante la SIC y ante otras Entidades externas, como por ejemplo las autoridades nacionales de ser el caso.

- Se debe seguir y dar cumplimiento al procedimiento de gestión de incidentes (Ver el documento Procedimiento de gestión de incidentes SC05-P01) para el manejo de incidentes que incluya los diferentes tipos: fallas en el sistema de información y pérdida del servicio, códigos maliciosos, denegación del servicio, errores debidos a datos del negocio incompletos o inexactos, violaciones de confidencialidad e integridad, uso inadecuado de sistemas de información, entre otros. Este procedimiento debe contemplar como mínimo las siguientes consideraciones:

  - Prevención con las diferentes herramientas de seguridad, con las que cuenta la entidad para la detección, evaluación y gestión de incidentes de seguridad que se puedan presentar.

  - Análisis e identificación del impacto de un incidente donde se vean comprometidos alguno de los tres pilares de la seguridad de la información Confidencialidad, Integridad o Disponibilidad

  - Definir acciones de contención, erradicación y recuperación, para evitar la recurrencia de los incidentes de seguridad. Asimismo, la comunicación con los afectados y el reporte de las acciones a la autoridad apropiada en caso de que sea necesario.

- Recolección, aseguramiento y documentación de las evidencias o rastros de los incidentes de seguridad, para el análisis y gestión, con el fin de tomar las medidas correctivas de posibles problemas internos, generación de evidencia forense con respecto a la violación de un contrato y/o legislación o para negociación de compensación de proveedores de software o servicios.

- El Oficial de Seguridad de la Información, o quien haga sus veces, es el encargado de liderar la solución al incidente de seguridad de la información.

- En el caso de que no se encuentre una solución que dé respuesta al incidente, el Oficial de Seguridad de la Información o a quien él delegue, puede contactar grupos de apoyo como autoridades, grupos de interés externos o foros que manejen asuntos relacionados a incidentes de seguridad de información para dar solución al mismo.

- El Oficial de Seguridad de la Información o a quien él delegue, debe desarrollar un plan de sensibilización para educar a los usuarios acerca de los incidentes de seguridad de la información, divulgando a quien se deben reportar, los tipos de incidentes, niveles de severidad y su implicación.

- La OTI a través del Oficial de Seguridad de la Información o a quien él delegue, debe cuantificar impactos de los incidentes de seguridad de la información, para determinar la prioridad de los mismos.

- La OTI a través del Oficial de Seguridad de la Información o a quien él delegue, debe contar con un registro de incidentes con sus respectivas soluciones que ayude a reducir el tiempo de respuesta en caso de ocurrencia de nuevos incidentes.

- La solicitud de inicio de un proceso legal está a cargo del Jefe de la OTI, del Oficial de Seguridad de la Información o quien ellos designen. La solicitud se debe presentar al responsable del Grupo de Trabajo de Control Disciplinario Interno de la Secretaría General de la SIC.El Oficial de Seguridad de la Información o a quien él delegue debe establecer relaciones con autoridades y otros grupos externos de apoyo en el caso que se considere necesario para atender un incidente de seguridad.

6.30 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Objetivo:

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

- Todos los servidores públicos, contratistas y terceros de la SIC deben conocer, acatar y cumplir, hacerse responsables de los actos que afecten la información y los datos de la Entidad, según lo estipulado en la ley 1273 del 2009 “Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- La Secretaría General a través del coordinador del Grupo de Trabajo de Control Disciplinario Interno o quien haga sus veces, debe aplicar el proceso disciplinario de la SIC, al incumplimiento y violación de las políticas de la seguridad de la información.

- La OTI a través del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, deben documentar todos los requerimientos legales y contractuales relacionados con la seguridad de la Información de la SIC, mediante la documentación del normograma del proceso de Gestión de la Seguridad de la Información.

6.31 DERECHOS DE PROPIEDAD INTELECTUAL

Objetivo:

Dar los lineamientos para proteger adecuadamente la propiedad intelectual propia como de terceros (derechos de autor de software o de documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros).

- No está permitido el uso de software duplicado y distribuido sin autorización (pirata).

- Todo el software que se utilice en los equipos de cómputo de la SIC, debe ser autorizado y debe contar con su respectiva licencia. Por ninguna circunstancia se permite el uso de software no licenciado. La autorización debe ser otorgada por la Jefatura de la Oficina de Tecnología e Informática o por el Oficial de Seguridad de la Información, siempre y cuando cumpla con los siguientes criterios:

  a) El software a instalar fue adquirido oficial y legalmente por la Entidad.

b) O el software cuenta con licencia GPL (Licencia Pública General – software libre).

c) O la licencia del software a instalar fue adquirida de forma personal por un servidor público, contratista y/o proveedor de la SIC y la requiere para dar cumplimiento a sus funciones u obligaciones contractuales.

El software será retirado por las siguientes razones:

- Por solicitud del propietario de la licencia.
- Por el vencimiento de tiempo de uso de la licencia.
- Por la desvinculación laboral o contractual del propietario de la licencia, con la SIC.

- Todo tipo de software, debe obtenerse de una fuente reconocida. Software obtenido de fuentes no confiables no debe ser utilizado en equipos a menos que sea autorizado por el Oficial de Seguridad de la Información o quien haga sus veces.

- La Oficina de Tecnología e Informática es la encargada de implementar las restricciones y limitaciones para la instalación de programas utilitarios en los equipos de cómputo de la SIC, en este sentido, solamente la mesa de servicios está autorizada para instalar software o programas utilitarios, con previa revisión de las condiciones de licenciamiento.

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, junto con el grupo de inventarios, debe mantener un inventario preciso de todo el software autorizado y se deben realizar controles internos periódicos para detectar productos sin licencia.

- La Dirección administrativa y la OTI deben contar con un inventario del licenciamiento corporativo de la SIC, con el fin de facilitar la revisión, administración y control de software no licenciado.

  En todos los contratos de la Entidad se debe establecer que la propiedad intelectual es exclusiva de la SIC, sobre cualquier material producido por los usuarios en desarrollo de sus funciones durante el tiempo de contratación.
- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe implementar controles para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.

- El material registrado con derechos de autor no se debe copiar total ni parcialmente, sin la autorización del propietario.

- No duplicar, convertir a otro formato o extraer registros comerciales (video, audio) más allá de lo que permita la ley de derechos de autor.

6.32 PROTECCIÓN DE REGISTROS

Objetivo:

Dar los lineamientos para la protección contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de los registros, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

- El Grupo de Trabajo de Gestión Documental y Archivo debe dar las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, protegerá los registros de eventos de seguridad de la información que se originen en la plataforma tecnológica de la SIC.

6.33 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES

Objetivo:

Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

La SIC define una política de tratamiento de datos personales, siendo el Oficial de Protección de Datos Personales el responsable en materia de seguridad de la información de:

1) Adelantar las investigaciones necesarias por las posibles violaciones a las normas legales vigentes de protección de datos personales, tanto por la SIC como Responsable de los datos, como frente a terceros como Encargados de los mismos.

2) Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las Políticas y Procedimientos en materia de Protección de Datos Personales.

3) Velar porque se capacite periódicamente en temas de protección de datos personales al personal del SGC, para generar una cultura de protección de datos dentro de la institución. Esto incluirá realizar sesiones de sensibilización y medir la participación y calificar el desempeño de los asistentes.

4) Integrar la Política de Tratamiento de Datos Personales dentro de las actividades de las demás áreas de la institución.

5) Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las Políticas y Procedimientos en materia de Protección de Datos Personales.

6) Coordina la realización de un análisis de riesgos anual de Protección de datos Personales de cada una de las áreas.

7) Apoyar la construcción de reglas sobre el uso responsable de la información, incluyendo controles de seguridad administrativos, físicos, tecnológicos, lógicos y jurídicos.

8) Realizar los reportes de incidentes de seguridad en el RNBD conforme a los parámetros establecidos en la Ley 1581 de 2012 y demás normas concordantes y vigentes.

6.34 POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Objetivo:

Garantizar que, ante un evento de contingencia o una situación de desastre, se debe mantener el estado actual de los controles que protegen la información crítica y sensible propia o en custodia de la Entidad.

- La OTI a través del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, en los casos que aplique, apoyará en las actividades de gestión de los riesgos asociados a la continuidad de los servicios críticos de TI.
- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá tomar las acciones tendientes a minimizar el impacto que se pudiera derivar de cualquier situación de emergencia sobre los servicios de TI identificados como críticos o el nivel de prestación de estos.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá tomar las acciones tendientes que permitan retornar al estado de normalidad en la infraestructura tecnológica afectada lo antes posible, una vez mitigadas las consecuencias del incidente perturbador.

- La OTI deberá tomar las acciones tendientes a fin de garantizar que el Plan de Recuperación ante Desastres, así como los correspondientes procedimientos técnicos requeridos, se desarrollan e implementan de forma adecuada, teniendo en cuenta los servicios y procesos críticos, tomando como referencia la evaluación de riesgos, su probabilidad e impacto.

- La OTI mantendrá actualizado en todo momento su Plan de Recuperación ante Desastres, con base en esto, se deben realizar revisiones periódicas y cada vez que se produzca un cambio significativo, ya sea en la infraestructura que soporta los procesos o en la normatividad aplicable que pueda afectar a los mismos.

- La OTI deberá tomar las acciones tendientes para garantizar la elaboración de los correspondientes documentos requeridos para el desarrollo de la continuidad del servicio de TI ante un desastre, asegurando que se mantengan actualizados los mismos.

- La OTI deberá gestionar los recursos necesarios para mantener el proceso de la continuidad del negocio en el sitio alterno, así como personal, proveedores y los planes requeridos que deben estar actualizados.

7 POLITICAS PARA EL LABORATORIO DE INFORMÁTICA FORENSE

7.1 POLÍTICA DE CONTROL DE ACCESO

Objetivo:

Prevenir y evitar el acceso no autorizado a las instalaciones, aplicativos, y demás activos de información de los cuales el Grupo de Trabajo de Informática Forense y Seguridad Digital - GTIFSD es propietario o mantenga su custodia.

7.1.1 Control de acceso lógico y gestión de privilegios para el laboratorio de informática forense

- El coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital, otorgará privilegios dentro de las plataformas de investigación forense y consulta web de la información recolectada por el GTIFSD, a los funcionarios y/o contratistas que hagan parte del GTIFSD y que sean designados por el

coordinador, para que estos efectúen las actividades de administración y capacitación en el buen uso de las plataformas.

Los permisos de acceso a las plataformas de investigación forense, serán autorizados por el coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital y únicamente se realizará la creación de usuario a los funcionarios y/o contratistas que cuenten con capacitación en el uso de las herramientas.

- Las cuentas de usuario de acceso a las plataformas de investigación forense y consulta web de la información recolectada por el GTIFSD, que alcancen un máximo de tres (3) intentos consecutivos sin éxito, serán bloqueadas. Los usuarios con cuentas bloqueadas, deberán solicitar la reactivación de la cuenta al coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital.

- El funcionario y/o contratista que requiera acceso a las plataformas forenses de revisión y consulta web desde ubicaciones diferentes a las instalaciones de la Superintendencia de Industria y Comercio, deberá ser autorizado mediante comunicación escrita por los Delegados de las diferentes áreas y/o Superintendente de Industria y Comercio.

- El coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien él delegue, debe verificar que los niveles de acceso (niveles de privilegios) a las plataformas forenses de revisión y consulta web asignados a los usuarios. Para ello, el administrador de cada plataforma de investigación forense y consulta web del GTIFSD, debe enviar un correo con el listado de los usuarios autorizados a los coordinadores, solicitándoles la confirmación o revocación de los permisos otorgados.

7.2 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo:

Proteger las áreas que contienen información y/o servicios de procesamiento de información del GTIFSD de la SIC.

7.2.1 Control de acceso físico

- El ingreso a las instalaciones donde se desarrollan actividades de laboratorio de Informática Forense de la SIC, es restringido únicamente al personal autorizado por el coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital. El acceso permanente se realizará mediante sistema biométrico; todo acceso temporal será tratado como visitantes, por ejemplo, funcionarios o contratistas de otras dependencias o proveedores

- Todos los visitantes a las instalaciones del Laboratorio de Informática Forense se deben registrar en la respectiva bitácora física antes de efectuar el ingreso y siempre deberán estar acompañados por algún miembro del personal del laboratorio forense, para lo cual se debe diligenciar el formato dispuesto para tal fin.

- El equipo de trabajo de Informática Forense de la SIC, debe tener un encargado, quien será responsable de administrar los elementos asignados, por ejemplo, cuarto de evidencias, caja fuerte, centro de cómputo, equipos forenses, entre otros.

7.2.2 Política de Uso Aceptable de Activos

- Los elementos del Laboratorio de Informática Forense únicamente pueden ser prestados y usados por los funcionarios y/o contratistas para propósitos relacionados con el cumplimiento de las funciones asignadas.

- Por ningún motivo, los funcionarios y contratistas asignados al Laboratorio de Informática Forense deben utilizar los elementos del mismo para propósitos personales.

7.2.3 Política de retiro de activos de información

- Los funcionarios o contratistas deben contar con la autorización del coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital para retirar activos de información de la SIC en calidad de préstamo.

- El retiro de los equipos forenses es exclusivamente para el desarrollo de las funciones de acompañamiento de visitas administrativas, audiencias y demás actividades de carácter de informática forense que requiera el área o dependencia solicitante.

- El retorno de los equipos forenses retirados en calidad de préstamo, deben ser devueltos al finalizar la atención de la visita administrativa, audiencia o demás actividades de carácter de informática forense, los cuales deben ser entregados al funcionario y/o contratista designado del Grupo de Trabajo de Informática Forense y Seguridad Digital.

7.2.3.1 Seguridad de equipos fuera de las instalaciones de Laboratorio de Informática Forense

- Cuando el equipo forense se devuelva al responsable del Grupo de Trabajo de Informática Forense y Seguridad Digital para reparación, mantenimiento etc., la información confidencial deberá ser respectivamente guardada en una copia de respaldo y borrada de forma segura.

  Los funcionarios y/o contratistas que desarrollan funciones de Informática Forense, cuentan con un disco duro externo para el almacenamiento de herramientas e información de carácter confidencial, por lo cual dicha información debe estar cifrada mediante herramientas criptográficas.
- Los funcionarios y/o contratistas que desarrollan funciones de informática Forense fuera de la Entidad, deben tener cifrado sus equipos de cómputo mediante el uso de la herramienta de windows BitLocker, la llave generada deberá ser reportada al coordinador del Grupo de Trabajo y almacenada en un repositorio destinado para tal fin.

- La Entidad cuenta con una póliza de todo riesgo la cual cubre todo el inventario de la Entidad, para lo cual en caso de que se materialice el riesgo de hurto, pérdida o daño, el integrante del grupo a quien se materializo el riesgo deberá seguir los lineamientos estipulados en el Instructivo para la reclamación en caso de Siniestro (GA02-I01) establecido por el Grupo de Trabajo de Servicios Administrativos y Recursos Físicos.

7.3 POLÍTICA DE GESTIÓN DE INCIDENTES

Objetivo:

Asegurar un enfoque consistente, rápido, efectivo y ordenado para la gestión de incidentes de seguridad del GTIFSD de La Superintendencia de Industria y Comercio.

- El coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital debe definir el alcance de los funcionarios y contratistas que cumplen actividades de Informática Forense, para que conozcan sus funciones dentro de los niveles de atención a solicitudes e incidentes.

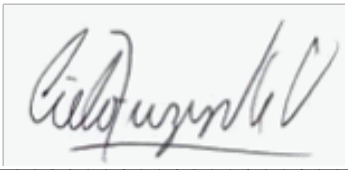
- El coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital debe escalar los incidentes al encargado para la atención de acuerdo con su criticidad y el responsable determinará las medidas preventivas o correctivas para su atención. Posteriormente informará al coordinador la solución empleada para dar respuesta al incidente.

- El Coordinador del Grupo de Trabajo de Informática Forense y Seguridad Digital debe programar una ventana de mantenimiento o una ventana de gestión de

cambio cuando sea necesario, el Profesional designado del Grupo de Trabajo de informática forense y seguridad digital registra el cambio por medio de la plataforma Aranda y diligencia los documentos necesarios ante la Oficina de Tecnología e Informática.

8 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

6.9.2 Gestión de usuarios novedades de personal SIC.
6.12 Política de controles de cifrado



CIELO ELAINNE RUSINQUE URREGO
Superintendente de Industria y Comercio
junio 2024