CONTENIDO

1. OBJETIVO

Establecer las políticas específicas de la seguridad de la información de la Superintendencia de Industria y Comercio, con el fin de regular la gestión de la seguridad de la información al interior de la entidad, protegiendo, preservando y administrando la integridad, confidencialidad y disponibilidad de la información.

2. DESTINATARIOS

Las políticas definidas en el presente documento deben ser conocidas y aplicadas por todos los macroprocesos estratégicos, misionales, apoyo y evaluación de la Superintendencia de Industria y Comercio, y por todos los servidores públicos y/o contratistas y terceros que tengan una vinculación laboral o acuerdos con la misma.

3. GLOSARIO

ACTIVO DE INFORMACIÓN: Cualquier cosa (Información Digital, Información Física, Software, Hardware, Servicio, Recurso Humano) que tenga valor para la organización.

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 en o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de 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.

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: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos.

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 de planear, coordinar y administrar los procesos de seguridad de la información en la organización.

OTI: Oficina de Tecnología e Informática.

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.

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. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un 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 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.

4. GENERALIDADES

La información, junto a los procesos, personas y sistemas que hacen uso de ella, es un activo que se considera esencial para las actividades de la Superintendencia de Industria y Comercio, y debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión de la información de la organización y que esté integrado con ellos, considerando la seguridad de la información en el diseño de procesos, sistemas de información y controles.

La Superintendencia de Industria y Comercio establecerá los mecanismos para respaldar la difusión, actualización y consolidación tanto de las presentes políticas como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión, para salvaguardar los derechos de los consumidores, proteger la libre y sana competencia, actuar como autoridad nacional de la propiedad industrial y defender los derechos fundamentales relacionados con la correcta administración de datos personales.

5. POLITICAS

5.1 Política de organización interna

Objetivo: Dar lineamientos para iniciar y 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 contenidas en este instructivo.

- El Comité Institucional de Gestión y Desempeño de la SIC, deliberará y aprobará las propuestas de implementación de medidas de seguridad de la información, cuya aplicación sea de carácter transversal a la operación de la Entidad.

- El Comité Institucional de Gestión y Desempeño de la SIC, revisará y aprobará el programa de cultura de seguridad de la información en la SIC.

- El Comité Institucional de Gestión y Desempeño de la SIC, debe acompañar e impulsar el desarrollo de proyectos de seguridad de la información.

- El Comité Institucional de Gestión y Desempeño de la SIC, debe aprobar el uso de metodologías y procesos específicos para la seguridad de la información.

- La OTI a través del 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, las encargadas de hacer cumplir la ley, los organismos de regulación y las autoridades de supervisión; también se incluyen las empresas de servicio públicos, los servicios de emergencia, los proveedores de electricidad y de salud y seguridad, por ejemplo, los departamentos de 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 agua (en relación con las instalaciones de enfriamiento de equipos).

- La OTI a través del Oficial de Seguridad de la Información o a quien él delegue, debe mantener los contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales para

compartir lecciones aprendidas en caso de que se presente un incidente de seguridad de la información, o 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 el cumplimiento de las políticas de seguridad de la información.

- La Oficina de Tecnología e Informática a través del 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.

5.2 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 de un proyecto. La gestión de riesgos será asesorada por el Oficial de Seguridad de la Información o a quien él delegue.

5.3 Política de seguridad para el teletrabajo

Objetivo: Proteger la información a la que se tiene acceso, es procesada o almacenada en un entorno de teletrabajo.

- Las políticas definidas en el presente instructivo, al igual que todas aquellas adicionales definidas por el Jefe de la Oficina de Tecnología e Informática de la SIC, se deben aplicar para los equipos de cómputo de teletrabajo.

- La navegación a internet desde equipos de teletrabajo se debe realizar siempre bajo la política de uso aceptable de activos de la SIC.

- Los teletrabajadores deberán aceptar y firmar el Acuerdo de Confidencialidad.

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

- El teletrabajador debe cumplir con las medidas de seguridad que la entidad ha implementado 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.

5.4 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.

5.4.1 Control antes de asumir el empleo

- El coordinador del Grupo de Trabajo del Talento Humano y el coordinador Grupo de Contratación deben verificar los antecedentes de todos los candidatos a un empleo de acuerdo con las leyes, reglamentos y ética pertinentes.

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

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

5.4.2 Términos y condiciones del empleo

- Todos los servidores públicos, contratistas y terceros a los que se brinde acceso a información confidencial, deberán firmar un acuerdo de confidencialidad, antes de tener acceso a las instalaciones de procesamiento de información.

- La SIC a través del coordinador del Grupo de Contratación y el coordinador del Grupo de Trabajo del Talento Humano deben asegurar de que los servidores públicos y/o, contratistas y terceros 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 organización 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 organización.

5.4.3 Durante la ejecución del empleo

- La SIC debe 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 deberán recibir la educación y/o formación para la toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización con respecto a la Seguridad de la Información.

5.4.4 Terminación y cambio de empleo

- El coordinador del Grupo de Trabajo del Talento Humano y el coordinador del Grupo de Contratación deben definir procedimientos para custodiar la información de la SIC, cuando se retire un servidor público o se termine la vinculación contractual con los contratistas.

- El coordinador del Grupo de Trabajo del Talento Humano y el coordinador del 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 confidencialidad o no divulgación, y las responsabilidades legales vigentes en el momento de la terminación laboral o contractual.

- El coordinador del Grupo de Trabajo del Talento Humano debe dar a conocer a servidores públicos los términos y condiciones del empleo que continúan después de un traslado.

- En el caso de un contratista suministrado a través de una parte externa, este proceso de terminación lo lleva a cabo dicha parte, de acuerdo con el contrato suscrito entre la organización y la parte externa.

- El coordinador del Grupo de Trabajo del Talento Humano y el coordinador del Grupo de Contratación informarán al jefe de la OTI acerca de los cambios de personal y de las disposiciones operativas.

- Se debe 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.

5.4.5 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 734 de 2002), 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 serán reportados ante la procuraduría y/o entidades competentes.

5.5 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 usuarios o custodios.

- Todos los servidores públicos y contratistas de la SIC, deben firmar un documento en el cual se comprometan a mantener los activos de información en condiciones adecuadas y a utilizarlos solamente para el desarrollo de las labores que le ha asignado la SIC.

- 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.

- La OTI debe implementar las medidas necesarias para la protección frente al riesgo debido a la utilización de equipos y comunicación móvil.

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

- Todos los requerimientos de aplicativos nuevos, y/o modificaciones a los existentes, deberán ser solicitados a la OTI.

- Los líderes de proceso deben remitir, vía correo electrónico, a la Mesa de Servicios, una solicitud identificando el usuario (interno o externo) al que se le deben habilitar los accesos a los recursos informáticos y tecnológicos, relacionando los servicios que requiera y el tiempo si es requerido.

- Los líderes de cada proceso o a quien él delegue, debe definir el tipo de acceso (lectura, escritura, modificación y borrado) y los roles sobre carpetas compartidas.

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

- Las salas de audiencia 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.

5.5.1 Uso de internet

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

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o a quien haga sus veces, dará autorización de uso solamente a los servicios de internet permitidos; es decir, los que puedan ofrecerse de manera segura.

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

- 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.

- No se debe acceder a páginas clasificadas con contenido pornográfico o no permitidas.

- No se debe instalar software que permita acceder a páginas o servicios no autorizados.

- 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

5.5.2 Uso de intranet (Intrasic)

- Los usuarios de la SIC utilizarán la intranet como un recurso de consulta de los documentos publicados.

- 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 responsable de cada área.

- Es responsabilidad del jefe de la Oficina de Servicios al Consumidor y Apoyo Empresarial a través del coordinador del Grupo de Comunicaciones, avalar la revisión y aprobación del material publicado.

- Es responsabilidad del jefe de la Oficina de Servicios al Consumidor y Apoyo Empresarial a través del coordinador del Grupo de Comunicaciones, depurar la información publicada.

- 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 uso de la intranet.

5.5.3 Uso de dispositivos móviles

- Todos los usuarios que tengan a su cargo dispositivos móviles institucionales se comprometen a hacer uso adecuado para el acceso a los servicios de la SIC.

- Los dispositivos móviles institucionales 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.

- Quienes tengan asignados dispositivos móviles institucionales, no deben desinstalar el software provisto en los mismos.

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

- Para todo dispositivo móvil institucional, se recomienda que posea 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, 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 tercero que requiera acceder a los servicios de la SIC desde su(s) dispositivo(s) móvil(es) personal(es) (correo electrónico, google drive, 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 SIC, a través de Oficina de Tecnología e Informática - OTI, podrá borrar todos los datos del dispositivo móvil de forma remota, siempre y cuando exista una solicitud escrita del propietario del dispositivo debidamente justificada (memorando o e-mail).

- La SIC, a través de Oficina de Tecnología e Informática - OTI, 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.

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

5.5.4 Uso del correo electrónico institucional

- El servicio de correo electrónico institucional es una herramienta para el intercambio de información exclusivamente laboral.

- 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 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 laborales 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 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.

- El usuario que envíe información propiedad de la SIC o de un tercero sin tener la autorización, responderá personalmente a medidas a nivel disciplinario y penal 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.

- Es responsabilidad del usuario hacer una administración periódica de su cuenta para evitar bloqueos por factores como el llenado de su buzón.

5.5.5 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. Bajo 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 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 SIC, brindando únicamente el servicio de internet, permitiendo únicamente el contenido aprobado en las políticas de seguridad de la SIC.

5.5.6 Uso del servicio de nube

- No está permitido almacenar información de la SIC en servicios de alojamiento de archivos multiplataforma en la nube (Dropbox, Onedrive, Box, Bitcasa, Mesa, icloud, entre otros similares) que no hayan sido autorizados por la OTI.

5.6 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 anualmente, o cuando se realiza actualizaciones al proceso al que pertenece el activo.

- La OTI a través de la coordinación del Grupo de Trabajo de Informática Forense y Seguridad Digital o quien haga sus veces, en conjunto con los líderes de los procesos de la SIC, identificará y valorará los activos de información que requieren de mayor protección para el cumplimiento misional de la entidad.

5.7 Política de devolución de activos de información

Objetivo: Todos los servidores públicos, contratistas y terceros 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 o terceros 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.

- Todos los servidores públicos, contratistas o terceros 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 que la información contenida no se pueda recuperar.

- 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 reubique a un servidor público en otra área, se debe instalar de nuevo el sistema operativo y demás programas básicos necesarios.

5.8 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 5.28 Política de borrado seguro en este documento).

- 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 que debe estar disponible por un periodo de tiempo mayor a la del medio removible, debe ser almacenada en otro medio, de manera que se asegure la confidencialidad, integridad y disponibilidad de la información.

- La información de carácter sensible que se disponga en un medio extraíble debe seguir un proceso de cifrado adecuado (Ver numeral 5.11 Política de controles de cifrado en este documento y el Instructivo de clasificación y rotulación de la información). 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 5.18 Política de control de código malicioso en este documento).

- Cuando se libera la información almacenada en medios removibles, se debe formatear el medio removible, 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 a 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.

5.9 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.

5.9.1 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 GS01-P05 procedimiento de creación, cancelación y actualización de cuentas de usuarios).

- 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.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe verificar cada seis (6) meses que los niveles de acceso (o también llamados niveles de privilegios) asignados a los usuarios sean apropiados de acuerdo al propósito del negocio y se conserve la separación de funciones.

- 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 usuario sea retirado o reasignado en sus funciones, el Grupo de Talento Humano debe informar a la Mesa de Servicios vía correo electrónico.

- En caso de que un contratista termine su contrato de forma anticipada, cada líder de proceso y/o supervisor debe informar al Jefe de la OTI, para bloquear inmediatamente los niveles de acceso que le hayan sido otorgados.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, debe verificar y retirar las cuentas redundantes de usuarios.

- Los servidores públicos y contratistas tienen prohibido usar la identidad de otro usuario, al hacer uso de los servicios y sistemas de información de la SIC.

- 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 5.10 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 5.32 - derechos de propiedad intelectual y 5.5 - política de uso aceptable de activos del presente documento, siendo responsables en caso de incumplimiento de las mismas.

5.10 Política de contraseñas

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

5.10.1 Contraseñas de usuario

- En el momento de la asignación de una contraseña a un usuario o a un grupo de usuarios, la mesa de servicios debe informar a los mismos sobre el carácter confidencial de ésta.

- Los usuarios pueden realizar el cambio de contraseña a través de la URL https://mail.sic.gov.co, en la opción recuperar contraseña.

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

- Las contraseñas no se deben almacenar en un computador en un formato no cifrado.

- Las contraseñas por defecto asociadas a un software o sistema de información deben ser cambiadas inmediatamente después de la instalación.

5.10.2 Selección y uso de contraseñas

- Todos los usuarios antes de acceder a un recurso de tecnología, tienen que identificarse y autenticarse por medio de un usuario y una contraseña.

- Los usuarios son responsables del uso de las contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos.

- Los usuarios deben mantener la confidencialidad de las contraseñas.

- Los usuarios no deben mantener registros de las contraseñas (hojas de papel, archivos digitales, 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 de puesta en peligro del sistema o a intervalos regulares, evitando la reutilización de contraseñas antiguas.

- Los usuarios deben seleccionar contraseñas con un mínimo de ocho (8) caracteres con las siguientes características:

  - Que sea alfanumérica (que contenga números, mayúsculas y minúsculas).
  - Que contenga caracteres especiales (#$%@/)

- Los usuarios no deben almacenar las contraseñas en un proceso de registro automatizado (plugin, extensión, macro, etc.).

- Los usuarios no deben compartir las contraseñas. La contraseña es personal e intransferible.

  - Los usuarios no se deben usar las mismas contraseñas para propósitos del negocio y para propósitos personales.

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

5.10.3 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 5.10.2).

- La contraseña debe cambiarse obligatoriamente cada 45 días, o cuando lo establezca el Jefe de la OTI, y ésta debe ser distinta a los 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 7 (siete) 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 funcionarios y contratistas de la entidad, deben crear contraseñas de calidad (ver Numeral 5.10.2) y evitar totalmente usar contraseñas como mayo2017 durante la atención a los usuarios, para lo anterior se puede hacer uso de herramientas generadoras de contraseñas.

5.11 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 al código fuente del programa y harán uso de la misma.

- 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.

5.12 Política de controles de cifrado

Objetivo: Proporcionar los lineamientos para proteger la confidencialidad, autenticidad 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 medios móviles o removibles o a través de líneas de comunicación. (Ver el Instructivo de clasificación y rotulación de la 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, 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).

5.13 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.

5.13.1 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 de Gestión Documental y Recursos Físicos.

- Cualquier ingreso de terceros a las instalaciones de la SIC de lunes a viernes después de las 5 p.m., debe ser avalado previamente por la Dirección Administrativa a través del coordinador de Gestión Documental 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 SC04-F28 - Reglamento de Higiene y Seguridad Industrial y SC04-F30 - 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.

5.13.1.1 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.

- Todas 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.

5.13.1.2 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.

5.13.2 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.

5.13.3 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.

5.13.4 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.

5.13.5 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 Gestión Documental 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.

5.13.6 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.

5.14 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.

5.14.1 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.

5.14.2 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.

5.15 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.

5.15.1 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.

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

5.15.2 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.

5.16 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.

5.16.1 Seguridad de equipos fuera de las instalaciones

- 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 (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 5.4 Política de Contraseñas en este documento).

5.17 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 Recursos Físicos, 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 Recursos Físicos, 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.

5.18 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.

- El CAB y ECAB deberá estar formado por el Jefe de la OTI, Coordinador de Infraestructura, Coordinador Proyectos Informáticos, Coordinador Sistemas de Información, Gestor de Cambios y/o por alguno de los siguientes roles:

  - ✓ Gestor de incidentes
  - ✓ Gestor de problemas
  - ✓ Gestor de Liberación y despliegue
  - ✓ Gestor de configuración y activos del servicio
  - ✓ Especialistas de cambios
  - ✓ Coordinador de cambios
  - ✓ Proveedor y/o representante
  - ✓ Clientes y/o usuarios

- El comité de cambios CAB se reunirá todos los miércoles, por lo cual todas las solicitudes de cambio sin excepción se reciben hasta el día martes antes de mediodía, si no se allega en ese tiempo, la solicitud quedará pendiente para ser revisada en el comité de la siguiente semana.

- 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.

- Todos los procesos de la SIC deben alinearse al proceso de Gestión de Cambios de tal manera que aseguren que sus cambios sean autorizados

- 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 GS02-P04 - Procedimiento de gestión del cambio tecnológico). 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.

5.19 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 control definidas en 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 GS01-P07 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.

5.20 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.

- 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 al formato GS01-F12 - Formato definición de backup de la Información.

- Todos los backups deben ser retenidos de acuerdo a 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.

- Se debe tener un registro del transporte de las copias de seguridad entre el Data Center externo y las instalaciones de la SIC.

- El encargado y custodio del transporte de las copias de seguridad entre el Data Center externo y las instalaciones de la SIC, será designado por el Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces.

- Se debe contar con el embalaje adecuado para proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito de las copias de seguridad.

- 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 5.29 - Política de gestión de incidentes en este documento).

- Los administradores de los aplicativos y sistemas de información, 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 o DVD), 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.

- Las copias de respaldo deberán estar protegidas por medio de cifrado. Para la realización del cifrado del backup, se debe seguir los pasos indicados en el

documento instructivo GS01-I05 Administración de seguridad de las copias de sistemas.

- Después de vencido el periodo de retención se debe eliminar el contenido los medios estándares de almacenamiento utilizados de acuerdo a las políticas y procedimientos aplicables (ver numeral 5.8 - 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 medios deben estar adecuadamente etiquetados de tal forma que sean fácilmente identificables. El etiquetado se debe realizar de la siguiente forma:

  Índice $_{backup}$ Tipo $_{backup}$ Fecha $_{ejecución}$ - Consecutivo

  Donde:

  - Índice $_{backup}$: Corresponde al índice de backup asignado en el documento GS01-F08 - Formato de definición de backups de la Información.
  - Tipo $_{backup}$: Corresponde al tipo de backup (T: Total, I : Incremental, D : Diferencial) asignado en el documento GS01-F08 - Formato de Definición de Backups de la Información.
  - Fecha $_{ejecución}$: Corresponde a la fecha de ejecución del backup en el formato: día/mes/año, por ejemplo: 01/02/17
  - Consecutivo: Número de consecutivo en caso de que se requiera más de un medio de almacenamiento para guardar el backup.

- 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.

- Es responsabilidad de los usuarios la información que resida en el computador asignado por la SIC, e identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

- 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.

5.21 Registro (logging) y seguimiento

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

5.21.1 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.

5.21.2 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.

5.21.3 Registros (logs) del administrador y del operador

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

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

5.21.4 Sincronización de relojes

- La OTI a través de quien delegue el coordinador del Grupo de Trabajo de Servicios Tecnológicos, debe sincronizar los relojes de los 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.

5.22 Política de auditorías de sistemas de información

Objetivo: Auditar 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 auditorías 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 auditoría.

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

- Las pruebas de auditoría 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 auditoría 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 de auditoría 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 auditorías de los sistemas de Información de la SIC, y éstos se deberán proteger y custodiar de accesos no autorizados.

5.23 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 trimestralmente.

- 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.

- Se debe documentar e informar los hallazgos de las vulnerabilidades técnicas, y las acciones apropiadas y oportunas realizadas para minimizar el nivel de riesgo.

- Dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se deberá llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información.

5.24 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.

5.24.1 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.

5.24.2 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.

5.24.3 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.

5.24.4 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, para 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.

5.25 Política de transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

5.25.1 Transferencia de información

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá contar con los lineamientos para proteger la información transferida contra interceptación, copiado, modificación, y destrucción.

- El usuario 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.

- La OTI a través del Grupo de Servicios Tecnológicos o quien haga sus veces, deberá establecer los 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.

- 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.

5.25.2 Acuerdos sobre transferencia de información

- El jefe de la OTI a través del Oficial de Seguridad de la Información, deberá establecer los lineamientos para proteger, controlar y notificar la transmisión, despacho y recibo de la información.

- El jefe de la OTI a través del Oficial de Seguridad de la Información, deberá establecer un acuerdo para la transferencia de información entre la SIC y las partes externas.

- Los datos e información creados, almacenados y recibidos, serán propiedad de la SIC, los usuarios solo podrán realizar copias de sus archivos personales; para copiar o 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.

5.25.3 Mensajería electrónica

- La OTI a través del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá proteger adecuadamente la información incluida en la mensajería electrónica.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos o quien haga sus veces, deberá dar aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información.

- No se debe utilizar canales de chat o grupos sociales como Facebook, Twitter, Youtube, Google+, etc., en horario laboral con fines personales, sin previa autorización.

- El grupo de comunicaciones será el responsable de manejar los canales de redes sociales con la imagen institucional de la entidad.

5.25.4 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, contratistas y terceros, 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.

5.26 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.

5.26.1 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 del Grupo de Sistemas de Información y Gestión de Proyectos Informáticos, deberá definir 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.

- 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 (se debe realizar una mezcla de los campos de los datos almacenados en las bases de datos de 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.

5.26.2 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.

- La copia de información de un entorno de producción a un entorno de prueba debe realizarse por medio de una autorización del Oficial de Seguridad de la Información.

- 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.

5.26.3 Política de desarrollo seguro

- La SIC aplicará una metodología que incluya los requerimientos de seguridad en todo el ciclo de vida de desarrollo y mantenimiento seguro de las aplicaciones, los desarrolladores revisarán y determinarán la acción a seguir para el tratamiento de las vulnerabilidades, para evitar que tengan brechas de seguridad, de otro lado, cuando el desarrollo es contratado a un tercero se deben definir acuerdos contractuales para asegurar el cumplimiento de los requerimientos de seguridad.

- En las aplicaciones a desarrollar se deben identificar y aplicar requisitos de seguridad de la información.

- Las pruebas a los sistemas deben incluir pruebas de seguridad de la información que busquen evitar, encontrar y resolver las vulnerabilidades.

- Los nuevos desarrollos o modificaciones a los existentes se deben probar y validar antes de ser puestos en producción.

5.27 Seguridad de la información en las relaciones con los proveedores

Objetivo: Establecer los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Superintendencia de Industria y Comercio.

- Los líderes de procesos únicamente deben proporcionar accesos a la información de la SIC a los proveedores, cuando se requiera para cumplir su objeto contractual.

- La dependencia contratante de la SIC deberá exigir a los proveedores los controles de exactitud y completitud, para asegurar la integridad de la información o del procesamiento de la información suministrada.

- La dependencia contratante de la SIC deberá solicitar apoyo a la OTI para definir los requisitos y controles de seguridad de la información se documentarán en los contratos.

- El coordinador del Grupo de Contratación deberá suministrar en las minutas de los contratos con terceros y proveedores, el espacio para definir los requisitos de seguridad de la información.

5.28 Gestión de la prestación de servicios de proveedores

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio con los proveedores que trabajan en la SIC.

5.28.1 Seguimiento y revisión de los servicios de los proveedores

- Cada supervisor de contrato debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

- Cada supervisor de contrato debe hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos.

- Cada supervisor de contrato debe revisar los reportes de servicio elaborados por el proveedor, y concertar reuniones de avance regulares, según se exija en los acuerdos.

5.28.2 Gestión de cambios en los servicios de los proveedores

- 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.

5.29 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.

- La OTI a través de la coordinación del Grupo de Trabajo de Servicios Tecnológicos, quien haga sus veces, es el encargado de aprobar una herramienta software para escanear el medio de almacenamiento y ejecutar un borrado seguro.

- La Mesa de Servicios es la encargada de aplicar el procedimiento de borrado seguro sobre un medio de almacenamiento y verificar que después de efectivamente no se pueden recuperar datos. Para esta actividad de verificación se debe usar una herramienta software de recuperación de datos.

- Los activos de información físicos que se encuentren en estado deteriorado y contengan información sensible deben ser sometidos a un análisis de riesgos que determine si es conveniente eliminar el activo o enviarlo a reparación.

- De no ser posible ejecutar el procedimiento de borrado seguro, se debe verificar si es posible destruir el medio.

- La coordinación del Grupo de Trabajo de Servicios Tecnológicos, o quien haga sus veces, es el encargado de informar al almacén de que dicho medio de almacenamiento debe ser destruido físicamente puesto que contiene información para la cual la SIC es propietario o custodio y no debe ser posible su recuperación por propósito de mantener la seguridad de la información.

- 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.

5.30 Política de gestión de incidentes

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 y contratistas 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 SC05-P01 - Procedimiento de gestión de incidentes) para el manejo de incidentes que incluya los diferentes tipos: fallas en el sistema de información y pérdida del servicio, códigos maliciosos, negación 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:

  - Contener un análisis e identificación del impacto del incidente (pérdida de confidencialidad, Integridad o Disponibilidad), la acción correctiva para evitar la recurrencia, la comunicación con los afectados y el reporte de la acción a la autoridad apropiada en caso de que sea necesario.

  - Hacer referencia hacia la recolección y aseguramiento de los rastros de los incidentes para: posibles análisis de problemas internos, generación de evidencia forense con respecto a la violación del contrato o de la legislación, o para negociación de compensación de proveedores de software o servicios.

- El Oficial de Seguridad de la Información o a quien él delegue, es el responsable de la gestión de incidentes de seguridad de la información.

- El Oficial de Seguridad de la Información, o quien haga sus veces, es el encargado de llevar a cabo la implementación de la solución al incidente.

- 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

- La OTI a través del Oficial de Seguridad de la Información o a quien él delegue, debe desarrollar un medio de aprendizaje 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 los tipos, volúmenes y costos de los incidentes de seguridad de la información, para hacer análisis de recurrencias de incidentes e impactos 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 Secretaria General de la SIC.

- La OTI a través del 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.

5.31 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 sus actos según lo indica 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".

- El incumplimiento y violación de las políticas de la seguridad de la información de la SIC, se les aplicará lo establecido en la ley.

- 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 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.

5.32 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.

- Los usuarios no deben ejecutar software que no haya sido instalado de acuerdo con el procedimiento de configuración de hardware y software (ver el documento GS01-P06 - Procedimiento de configuración de hardware y software.)

- 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. (Ver el documento GS01-P06 - Procedimiento de configuración de hardware y software).

- 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.

- El grupo de inventarios y la OTI debe contar con un inventario del licenciamiento corporativo de la SIC, con el fin de facilitar la revisión, administración y control de software no licenciado.

- Son de propiedad exclusiva de la SIC, 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 de registros comerciales (video, audio) más allá de lo que permita la ley de derechos de autor.

5.33 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 Recursos Físicos debe dar las directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información.

- El Grupo de Trabajo de Gestión Documental y Recursos Físicos debe establecer e implementar controles para proteger los registros contra pérdida, destrucción y falsificación.

- 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.

5.34 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 y adelantará las investigaciones necesarias por las posibles violaciones a las normas legales vigentes de protección de datos personales, de acuerdo con el procedimiento PD01-P01 Procedimiento de Investigaciones sobre posibles violaciones a las normas sobre protección de datos personales.

5.35 Revisiones de seguridad de la información

Objetivo: Establecer los lineamientos para asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

- El Jefe de la OTI a través del Oficial de Seguridad de la Información o quien haga sus veces, realizará acciones de verificación del cumplimiento del Instructivo Políticas del Sistema de Gestión de Seguridad de la Información - SGSI.

- Los líderes de los procesos de la SIC deben apoyar las revisiones del cumplimiento de los sistemas con las políticas, normas y procedimientos de seguridad apropiados y cualquier otro requerimiento de seguridad.

6. DOCUMENTOS RELACIONADOS

A- GS01-P05 Procedimiento de creación, cancelación y actualización de cuentas

	de usuarios.
B - GS01-P07	Procedimiento de instalación de parches de seguridad.
C - SC05-P01	Procedimiento de gestión de incidentes.
D - GS01-P08	Procedimiento de gestión del cambio tecnológico.
E - GS01-I05	Administración de seguridad de las copias de sistemas.
F -	Procedimiento de borrado seguro.
G - SC04-F28	Reglamento de higiene y seguridad industrial.
H - SC04-F30	Plan de emergencias.
I -	Instructivo de clasificación y rotulación de la información.

7. RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Se adicionan lineamientos en la política 5.9.1 - Control de acceso lógico y gestión de privilegios. Se adicionan lineamientos en la política 5.32 Derechos de propiedad intelectual. Se adicionan lineamientos en la política 5.25.1 Transferencia de información. Se ajustan las políticas 5.10.3 Gestión de contraseñas. Se realiza cambio de código documental debido al cambio de proceso, siendo el código anterior GS02-I06. Se reasignan las responsabilidades entre el Grupo de Trabajo de Servicios Tecnológicos y el Grupo de Trabajo de Informática Forense y Seguridad Digital.

Fin documento