SUPERINTENDENCIA DE ORDENAMIENTO TERRITORIAL, USO Y GESTIÓN DEL SUELO

Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales - CGDIG

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA SUPERINTENDENCIA DE ORDENAMIENTO TERRITORIAL, USO Y GESTIÓN DEL SUELO

2018 - 2022

Control del Documento				
Elaborado por:	**Cargo**	**Versión:**	**Fecha:**	**Firma**
Ing. Mónica Uyana García	Coordinadora General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG)	1.0	30 de marzo de 2018	
Actualizado por:	**Cargo**	**Versión:**	**Fecha:**	
Ing. Mónica Uyana García	Coordinadora General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG)	1.1	03 de julio de 2018	
Aprobado por:	**Cargo**	**Versión:**	**Fecha:**	
Arq. Fernando Pauta Calle	Superintendente de Ordenamiento Territorial, Uso y Gestión del Suelo (Subrogante)	1.1	06 de julio de 2018	

ÍNDICE:

1. INTRODUCCIÓN

La Política de Seguridad de la Información de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo (SOT), constituye el marco de referencia orientado a establecer directrices de gestión, mediante un enfoque informativo, preventivo, y reactivo como instrumento de conocimiento, aplicación y concientización para los funcionarios, proveedores y terceros, independiente del cargo que desempeñen.

La presente Política está orientada a la Gestión de la Seguridad de la Información de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo (SOT), y sus oficinas zonales a nivel nacional, tomando como base la Norma ISO/IEC 27001:2013, para garantizar la Confidencialidad, Integridad y Disponibilidad de la información, protección y resguardo de las personas y activos, así como aseguramiento de la disponibilidad de los recursos de la Institución.

2. OBJETIVOS

La presente Política tiene por objetivo crear las bases y lineamientos necesarios para proteger la información y sus activos relacionados, de riesgos y amenazas deliberadas o accidentales, con el fin de mantener los niveles de Confidencialidad, Integridad y Disponibilidad establecidos para el cuidado de los datos e información de la Institución, así como de los recursos informáticos que operan en sus instalaciones, o que estén alojados y administrados por terceros u otro proveedor de servicios contratados.

- Cumplir con las leyes, regulaciones y normativas vigentes relacionadas con los servicios provistos por la Institución para sus usuarios.
- Proporcionar lineamientos y principios sobre los cuales debe asentarse la Seguridad de la Información de la Institución, en concordancia con las estrategias y objetivos del basados en la Filosofía, Propósito y Valores de SOT.
- Establecer y mantener criterios para el manejo de riesgos en Seguridad de la Información.
- Disponer de un área de Seguridad de la Información consolidada que se encargue de asegurar la información y definir los lineamientos necesarios para la protección de los recursos informáticos de eventos como destrucción, alteración o accesos no autorizados, mediante el empleo de controles de seguridad.
- Disponer y asignar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente la Gestión de Seguridad de la Información en la Institución.
- Registrar e investigar todas las violaciones a la Política y lineamientos de Seguridad de la Información.
- Gestionar los incidentes de Seguridad de la Información de forma adecuada en base a los resultados de las evaluaciones de riesgos asociados a la pérdida de Confidencialidad, Integridad y Disponibilidad de la información y de los sistemas

de información de riesgos y amenazas que atenten contra los procesos vitales de SOT.

- Disponer de un Sistema de Gestión de Continuidad del Negocio (SGCN), integral que permita mitigar, reducir, transferir y/o aceptar los riesgos identificados con el fin de garantizar la continuidad del negocio ante la suscitación de eventos adversos, desastres o indisponibilidad de los servicios y/o sistemas propios de la Institución o contratados.
- Evaluar los controles de seguridad, y efectividad frente a la mitigación de los riesgos identificados, considerando el nivel de exposición a los riesgos.
- Informar, comunicar y concientizar a los funcionarios, proveedores y terceros, las obligaciones del cumplimiento de la presente Política de Seguridad de la Información.

3. ALCANCE

La presente Política de Seguridad de la Información, denota el compromiso de la Alta Dirección para el establecimiento de un Comité de Seguridad de la Información, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información para la SOT, con el fin de garantizar la protección de sus funcionarios, información y activos relacionados.

La presente Política es aplicable a toda la SOT. No se permitirán excepciones, excepto circunstancias especiales previamente analizadas y evaluadas por el área de Seguridad de la Información quién recomendará en el caso de ser favorable la autorización por parte del Comité de Seguridad de la Información o representante, quien mantendrá y retendrá la documentación de soporte durante el tiempo necesario.

4. PRINCIPIOS Y NORMAS ESPECÍFICAS

4.1 Términos y Definiciones

Para el propósito del presente documento, se aplican los términos y definiciones dados en ISO/IEC 27000.

4.2 Contexto de la Institución

SOT debe determinar los asuntos internos y externos que sean relevantes para su propósito y que afectan su capacidad para lograr el o los resultados esperados del Sistema de Gestión de la Institución, para lo cual debe determinar:

- Las partes interesadas que sean relevantes para el Sistema de Gestión de la Seguridad de la Información.
- Los requisitos de las partes interesadas con respecto a la Seguridad de la Información.

4.3 Determinación del alcance del Sistema de Seguridad de la Información

SOT debe determinar los límites y la aplicabilidad del Sistema de Seguridad de la Información para establecer su alcance, considerando:

- Los asuntos internos y externos.
- Las necesidades y expectativas de las partes interesadas.
- Las interfaces y dependencias entre las actividades desempeñadas por la Institución y aquellas que desarrollan otras Organizaciones.

4.4 Sistema de Gestión de Seguridad de la Información

SOT debe establecer, implementar, mantener y mejorar de manera continua el Sistema de Seguridad de la Información, de acuerdo a los requisitos de la Norma Internacional ISO/IEC 27001:2013.

4.5 Liderazgo y Compromiso

La Alta Dirección deberá demostrar liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información mediante las siguientes acciones:

- Garantizando el establecimiento de la Política y objetivos de la Seguridad de la Información y que estos sean compatibles con la dirección estratégica de SOT.
- Garantizar la integración de los requisitos del Sistema de Gestión de la Información dentro de los procesos de la Institución.
- Garantizar la disponibilidad de los recursos necesarios para el Sistema de Gestión de la Seguridad de la Información.
- Comunicar la importancia de una gestión efectiva de Seguridad de la Información y de adecuarse a los requisitos del Sistema de Gestión de la Seguridad de la Información.
- Garantizar que el sistema de seguridad de la información logre los resultados esperados.
- Dirigir y dar soporte a las personas para que contribuyan con la efectividad del Sistema de Gestión de la Seguridad de la Información.
- Promover la mejora continua.
- Apoyar las funciones de la Gerencia que permitan demostrar su liderazgo siempre que corresponda a sus áreas de responsabilidad.

4.6 Política

La Política de Seguridad de la Información de SOT debe estar disponible como información documentada, ser comunicada dentro de la Institución, y estar disponible para las partes interesadas de la manera que estimen adecuada.

4.7 Funciones, responsabilidades y autoridad de la Institución

La Alta Dirección debe garantizar que se asigne y comuniquen las responsabilidades y autoridad para los roles relacionados con la Seguridad de la Información, asignando la responsabilidad y autoridad para:

- Garantizar que el Sistema de Gestión de Seguridad de la Información se adapte a los requisitos de la Norma Internacional ISO/IEC 27001:2013.
- Informar acerca del desempeño del Sistema de Gestión de Seguridad de la Información a la Alta Dirección.

4.8 Acciones para enfrentar los riesgos y las oportunidades

SOT al planificar el Sistema de Gestión de la Seguridad de la Información debe considerar el Contexto de la Institución, necesidades, expectativas de las partes interesadas, y determinar los riesgos y oportunidades que deben orientarse a:

- Garantizar que el Sistema de Gestión de Seguridad de la Información logre los resultados esperados.
- Evitar o reducir efectos indeseados.
- Lograr la mejora continua.
- Planificar las acciones destinadas a manejar los riesgos y oportunidades.
- Buscar la manera para integrar e implementar las acciones dentro de los procesos del Sistema de Gestión de Seguridad de la Información.
- Evaluar la efectividad de estas acciones.

4.9 Evaluación de los Riesgos de Seguridad de la Información

La SOT debe llevar a cabo evaluaciones de los riesgos de Seguridad de la Información a intervalos planificados o cuando se proponen o se dan cambios, considerando la evaluación de los riesgos de Seguridad de la Información, y definiendo y aplicando el proceso de evaluación de los riesgos de Seguridad de la Información de modo que permita:

- Establecer y mantener los criterios de los riesgos de Seguridad de la Información, incluyendo los criterios de aceptación del riesgo, y los criterios para el desempeño de las evaluaciones de los riesgos de la Seguridad de la Información.
- Garantizar que la repetición de la evaluación repetitiva de los riesgos de la Seguridad de la Información arroje resultados válidos, consistentes y comparativos.
- Identificar los riesgos de Seguridad de la Información.
- Aplicar los procesos de evaluación de los riesgos de Seguridad de la Información para identificar los riesgos asociados a la pérdida de la confidencialidad,

integridad y disponibilidad de la información dentro del alcance del Sistema de Gestión de Seguridad de la Información.
- Identificar a los originadores de los riesgos.
- Analizar los riesgos de Seguridad de la Información, evaluando las consecuencias potenciales que se producirían si los riesgos identificados llegaran a materializarse.
- Evaluar la probabilidad realista de la ocurrencia de los riesgos identificados.
- Determinar los niveles de riesgo.
- Evaluar los riesgos de la Seguridad de la Información.
- Comparar los resultados del análisis de riesgos con los criterios de riesgos establecidos.
- Priorizar los riesgos analizados para el tratamiento de los riesgos.

La SOT debe conservar la información documentada acerca del proceso de evaluación de la Seguridad de la Información.

4.10 Tratamiento de los Riesgos de la Seguridad de la Información

SOT debe implementar el plan de tratamiento de los riesgos de Seguridad de la Información y definir y aplicar procesos de tratamiento de riesgos de la Seguridad de la Información con la finalidad de:

- Seleccionar las opciones de tratamiento de los riesgos de Seguridad de la Información, considerando los resultados de la evaluación de los riesgos.
- Determinar los controles que son necesarios para implementar las opciones seleccionadas para el tratamiento de la Seguridad de la Información.
- Comparar los controles determinados del Anexo A de la Norma, y verificar que no se encuentren omitidos controles que sean de utilidad.
- Elaborar una declaración de aplicabilidad que contenga los controles necesarios del Anexo A de la Norma, y la argumentación de las inclusiones o exclusiones.
- Formular el tratamiento de los riesgos de Seguridad de la Información.
- Hacer que los poseedores del riesgo aprueben el plan de tratamiento de riesgos de la Seguridad de la Información, y aceptar los riesgos residuales.

La SOT debe conservar la información documentada acerca del proceso de tratamiento de los riesgos de la Seguridad de la Información.

4.11 Objetivos de la Seguridad de la Información y la planificación para alcanzarlos

SOT debe establecer los objetivos de Seguridad de la Información en relación a las funciones y niveles. Los objetivos de Seguridad de la Información deben:
- Ser consistentes con la Política de Seguridad de la Información.
- Ser medibles (si es aplicable).

- Considerar los requisitos de Seguridad de la Información y los resultados de la evaluación de riesgos y del tratamiento de riesgos.
- Ser comunicados.
- Actualizados, si así lo requiriera.

SOT debe conservar la información documentada sobre los objetivos de la Seguridad de la Información. Al planificar cómo alcanzar sus objetivos de Seguridad de la Información la Institución debe determinar:

- Qué deberá hacer.
- Qué recursos necesitará.
- Quién será el responsable.
- Cuándo será alcanzado dicho objetivo.
- Cómo medirá los resultados.

4.12 Recursos

La SOT debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Información.

4.13 Competencias

La SOT debe:

- Determinar las competencias necesarias de las personas que harán el trabajo bajo su control, el mismo que afectará el desempeño de su Seguridad de la Información.
- Garantizar que las personas tengan una competencia en base a una educación, entrenamiento y experiencia adecuados.
- Si fuera el caso, llevar acciones que permitan adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas.
- Conservar una adecuada documentación de la información como evidencia de la competencia.

4.14 Concientización

Las personas que hacen el trabajo bajo el control de SOT deben ser conscientes de:

- La Política de Seguridad de la Información.
- Su contribución a la efectividad del Sistema de Gestión de la Seguridad de la Información incluyendo los beneficios de la mejora en el desempeño de la Seguridad de la Información.

- Las implicancias de la no conformidad con los requisitos del Sistema de Gestión de la Seguridad de la Información.

4.15 Comunicación

SOT debe determinar la necesidad de las comunicaciones internas y externas con respecto al Sistema de Gestión de Seguridad de la Información incluyendo:

- Qué se debe comunicar.
- Cuándo se debe comunicar.
- Con quién se debe comunicar.
- Quién debe comunicar.
- El proceso por el cual se debe hacer efectiva la comunicación.

4.16 Documentación de la Información

El Sistema de Gestión de la Información debe incluir:

- La documentación de la información requerida por la Norma Internacional.
- La documentación de la información determinada por la Institución como necesaria para la efectividad del Sistema de Gestión de la Seguridad de la Información.
- El tamaño de la Institución y su tipo de actividades, procesos, productos y servicios.
- La complejidad de los procesos y sus interacciones.
- Las competencias de las personas.

Al crear y actualizar la información documentada, la SOT debe garantizar una apropiada:

- Identificación y descripción de los documentos.
- Formato.
- Revisión y aprobación para una debida adecuación e idoneidad.

4.17 Control de la Información documentada

La información documentada requerida por el Sistema de Gestión de Seguridad de la Información y por la Norma Internacional debe ser controlada para garantizar:

- La disponibilidad e idoneidad para su uso, donde y en el momento que sea necesario.
- Adecuada protección que evite la pérdida de confidencialidad, uso inadecuado o pérdida de integridad.

Para el control de la información documentada la SOT debe desarrollar las siguientes actividades, según correspondan:

- Distribución, acceso, recuperación y uso.
- Almacenamiento y conservación, incluyendo la conservación de la legibilidad.
- Control de Cambios.
- Retención y disposición.

La SOT debe identificar y controlar en la medida de lo posible la información documentada de origen externo, determinado por la Institución como necesaria para la planificación y operación del Sistema de Gestión de la Seguridad de la Información.

4.18 Planificación y control operacional

La SOT debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de la Seguridad de la Información e implementar acciones para enfrentar los riegos y las oportunidades, también debe implementar planes para lograr los objetivos de Seguridad de la Información.

La SOT debe mantener información documentada de forma que garantice que se están llevando a cabo los procesos de acuerdo a lo planificado, y mantener un control sobre los cambios planificados y revisar las consecuencias de los cambios involuntarios, tomando acciones para mitigar cualquier efecto adverso, si el caso así lo amerita. La Institución debe garantizar, identificar y controlar todos los procesos tercearizados.

4.19 Acciones para enfrentar los riesgos y las oportunidades

En la SOT, al planificar el Sistema de Gestión de Seguridad de la Información se deben determinar los riesgos y oportunidades orientados a garantizar que el SGSI logre los resultados esperados, evitar o reducir efectos indeseados, y lograr la mejora continua.

4.20 Evaluación del Desempeño

La SOT debe evaluar el desempeño de la Seguridad de la Información y la efectividad del Sistema de Gestión de la Información, para lo cual debe determinar:

- Qué necesidades deben ser monitoreadas y sometidas a medición, incluyendo los procesos y controles de la Seguridad de la Información.
- Los métodos de monitoreo, medición, análisis y evaluación, según corresponda con la finalidad de garantizar la validez de los resultados.
- Cuándo debe ejecutarse el monitoreo y medición.
- Quién debe realizar el monitoreo y medición.
- Cuándo debe analizarse y evaluarse los resultados del monitoreo y de la medición.
- Quién debe analizar y evaluar los resultados.

La SOT debe conservar adecuadamente la información documentada como evidencia de los resultados del monitoreo y la medición.

4.21 Auditorías Internas

La SOT debe dirigir auditorías internas en intervalos planificados con la finalidad de proporcionar información con respecto a que si el Sistema de Gestión de la Seguridad de la Información se ajusta a:

- Los propios requisitos de la Institución con respecto al Sistema de Gestión de la Información.
- Los requisitos de la Norma Internacional.
- Se implementa y mantiene de manera efectiva.

La SOT debe planificar, establecer, implementar y mantener un programa o programas, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación y reporte.

El o los programas deben considerar la importancia de los procesos involucrados y los resultados de auditorías previas.

- Definir los criterios y alcance de la auditoría.
- Seleccionar auditores y dirigir auditorías que aseguren la objetividad e imparcialidad del proceso auditor.
- Garantizar que los resultados de la auditoría sean informados a la Gerencia correspondiente.
- Conservar información documentada como evidencia del o de los programas y los resultados de la auditoría.

4.22 Revisión por parte de la Alta Dirección

La Alta Dirección debe revisar el Sistema de Gestión de Seguridad de la Información a intervalos establecidos para garantizar su continua disponibilidad, adecuación y efectividad. La revisión debe incluir:

- El estatus de las acciones de las anteriores revisiones por parte de la Alta Dirección.
- Cambios en los asuntos externos e internos que tuvieron relevancia para el Sistema de Gestión de la Seguridad de la Información.
- Retroalimentación sobre el desempeño de la Seguridad de la Información, incluyendo la tendencia en las no conformidades y acciones correctivas, resultados del monitoreo de medición, y resultados de auditoría.
- Cumplimiento de los objetivos de Seguridad de la Información.
- Retroalimentación por parte de las partes interesadas.

- Resultados de la evaluación de los riesgos y estatus del plan de tratamiento de riesgos.
- Oportunidades de mejora continua

Los resultados de las revisiones por parte de la Alta Dirección deben incluir las decisiones con respecto a las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de Gestión de Seguridad de la Información.

La SOT debe conservar la información documentada como evidencia de los resultados de las revisiones por parte de la Alta Dirección.

4.23 Mejora (No conformidad y Acción correctiva)

La SOT ante una no conformidad debe:

- Reaccionar hacia la no conformidad.
- Tomar acciones para controlar y corregirla.
- Lidear con las consecuencias.
- Evaluar la necesidad de acción para eliminar las causas de la no conformidad, con la finalidad de evitar la recurrencia o la ocurrencia en cualquier otro lugar mediante:
    - La revisión de la no conformidad.
    - La determinación de las causas de la no conformidad.
    - La verificación de si existe no conformidad similar o podría darse.
    - La implementación de una acción necesaria.
    - La revisión de la efectividad de las acciones correctivas tomadas.
    - La implementación de cambios al Sistema de Gestión de Seguridad de la Información, si fuera necesario.

Las acciones correctivas deben estar acorde a los efectos de las no conformidades encontradas. La SOT debe conservar la información documentada como evidencia de:

- La naturaleza de las no conformidades y cualquier acción tomada posteriormente.
- Los resultados de las acciones correctivas.

4.24 Mejora Continua

La SOT debe mejorar de manera continua la idoneidad, adecuación y efectividad del Sistema de Gestión de la Seguridad de la Información.

4.25 Gestión de la Alta Dirección para la Seguridad de la Información

La Alta Dirección debe revisar, aprobar, y autorizar la publicación y comunicación de la Política de Seguridad de la Información a los funcionarios de la Institución y partes interesadas, la cual debe ser revisada en períodos regulares establecidos por el Comité

de Seguridad de la Información para la identificación de posibles cambios significativos y/o mejoras con el fin de garantizar su idoneidad, adecuación y efectividad continua.

4.26 Institución de la Seguridad de la Información

Para una adecuada administración de la seguridad, SOT contará con un área dedicada a velar por el cumplimiento de la presente Política con roles y responsabilidades claramente establecidos en Seguridad de la Información, la que deberá mantener contacto con la Alta Dirección y Comité de Seguridad de la Información y/o autoridades respectivas para el reporte de incidentes, recomendaciones de mejora y/o requerimientos en seguridad.

4.26.1 Segregación de tareas

Las tareas o áreas de responsabilidad en conflicto deben ser segregadas para reducir las oportunidades de modificación no autorizadas, involuntarias de información, o para evitar el uso inadecuado de los activos de la Institución. La posibilidad de colusión debe ser considerada en el diseño de los controles.

Los funcionarios con responsabilidades de Seguridad de la Información asignadas, podrán delegar tareas de seguridad a los demás. No obstante siguen siendo responsables y deben determinar que las tareas delegadas fueron realizadas correctamente.

4.26.2 Contacto con las Autoridades

Contar con procedimientos que especifiquen las responsabilidades de la persona designada para el contacto en caso de identificar incidentes de seguridad que atenten contra la Institución y que deban ser informados de manera oportuna a las Autoridades respectivas.

4.26.3 Contacto con Grupos Especiales de Interés

La Institución interna de la Seguridad de la Información debe mantener contacto con grupos especiales de interés, fórums y asociaciones de profesionales especializados en seguridad a fin de:

- Mejorar el conocimiento sobre las mejores prácticas y estar al día con la información de seguridad pertinente.
- Asegurar la importancia y comprensión de la Seguridad de la Información en la SOT.
- Recibir alertas tempranas, avisos y revisiones relacionados con los ataques y vulnerabilidades.
- Acceder a los consejos de Seguridad de la Información especializados.

- Comunicar e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Proporcionar puntos de enlace adecuados cuando se trata de incidentes de Seguridad de la Información.

4.26.4 Seguridad de la Información en la Gestión de Proyectos

La Seguridad de la Información debe adaptarse a la gestión de los proyectos, independientemente del tipo de proyecto.

4.27 Equipos móviles y trabajos a distancia

Garantizar la seguridad del trabajo a distancia, adoptando políticas y medidas de seguridad aplicables para los funcionarios de SOT, proveedores y terceros para el manejo de los riesgos derivados del uso de equipos móviles para el trabajo remoto, así como para los dispositivos y tecnologías móviles que facilitan la operación de la Institución en sus diferentes unidades de negocio.

Implementar medidas de seguridad para proteger la información a la que se accede, procesa o almacena en lugares de trabajo a distancia.

4.28 Seguridad de los Recursos Humanos

4.28.1 Filtración

Llevar a cabo la verificación de los antecedentes de datos e información proporcionada por los funcionarios, proveedores y terceros de acuerdo a las Leyes, regulaciones vigentes y a la ética, antes de la contratación, con el fin de crear un ambiente de trabajo seguro en la Institución.

4.28.2 Términos y Condiciones de Empleo

Los contratos y acuerdos contractuales con los colabores, proveedores y terceros deben fijar sus responsabilidades y las de la SOT con respecto a la Seguridad de la Información.

4.28.3 Responsabilidades de la Gerencia

Las Gerencias deben instar a los funcionarios y contratistas que desempeñan funciones en sus áreas, a aplicar la Seguridad de la Información de acuerdo a las Políticas y procedimientos establecidos por la Institución.

4.28.4 Concientización, educación y capacitación sobre Seguridad de la Información

Los funcionarios de la Institución y contratistas, si así lo requiriesen, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las Políticas y procedimientos organizacionales, de acuerdo a las

funciones de trabajo que desempeñen, para su cumplimiento con el fin de proteger los intereses de la SOT y de las personas durante y después del término del contrato.

4.28.5 Procesos disciplinarios

En la SOT deben existir procesos disciplinarios formales comunicados en la Institución, para ser aplicados en caso de requerirse la toma de acciones contra los funcionarios que cometan alguna infracción contra la Seguridad de la Información.

4.28.6 Término o cambio de responsabilidades de empleo

La SOT debe definir, comunicar y reforzar a todos los funcionarios y contratistas, las responsabilidades y tareas de Seguridad de la Información que permanecerán válidos después del término del empleo.

4.29 Gestión de los Activos

En la Institución se deben identificar los activos y definir las responsabilidades adecuadas de protección.

4.29.1 Inventario de los activos

Los activos e información de la SOT deben ser identificados, inventariados, clasificados y controlados de manera apropiada.

4.29.2 Uso aceptable de los activos

Los activos deben ser asignados a un responsable o "custodio", para su resguardo, cuidado y protección, empleando controles y reglas de seguridad para el uso aceptable de los activos, información e instalaciones, los mismos que permitan minimizar los riesgos de daños, interrupciones de servicios, divulgación de información, entre otros.

4.29.3 Retorno de los activos

Todos los funcionarios internos y externos deberán devolver los activos que estén en su posesión una vez finalizado su empleo, contrato o acuerdo.

4.30 Clasificación de la Información

Garantizar que la información de SOT reciba un nivel adecuado de clasificación, protección y etiquetado de acuerdo a los niveles de clasificación establecidos, previniendo los accesos no autorizados, divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los activos de información y/o medios de comunicación.

4.30.1 Clasificación de la Información

La información debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.

4.30.2 Etiquetado de la Información

La SOT debe desarrollar e implementar una serie de procedimientos adecuados para el etiquetado de la información, acorde al esquema de clasificación de la información adoptado por la Institución.

4.30.3 Manejo de activos

La SOT debe desarrollar e implementar procedimientos de manejo de los activos de acuerdo al esquema de clasificación de la información adoptado por la Institución.

4.31 Manejo de los Medios de Comunicación

La SOT debe prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de comunicación.

4.31.1 Gestión de los Medios de Comunicación Removibles

Se debe implementar procedimientos para la gestión de los medios de comunicación removibles de acuerdo al esquema de clasificación adoptado por la Institución.

4.31.2 Disposición de los Medios de Comunicación

Los medios de comunicación deben ser desechados de manera segura cuando ya no son necesarios, mediante procedimientos formales.

4.31.3 Transferencia física de los Medios de Comunicación

Los medios de comunicación que contienen información deben ser protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte.

4.32 Control de Acceso

Los accesos a la información y recursos de información deben ser concedidos de manera controlada garantizando el ingreso a los servicios de red, información, sistemas, servicios, aplicaciones, entre otros recursos de la SOT, únicamente a los funcionarios y/o

partes interesadas autorizadas, quienes serán responsables de salvaguardar la autenticidad de su información y claves de acceso.

4.32.1 Acceso a las redes y a los servicios de las redes

Los usuarios de la SOT deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar.

4.33 Gestión del Acceso al Usuario

Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios de SOT.

4.33.1 Registros y des-registros

La SOT debe implementar procesos de registro y des-registro de usuarios para habilitar los derechos de acceso.

4.33.2 Provisión de Acceso al Usuario

La SOT debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.

4.33.3 Gestión de los derechos de acceso privilegiado

La SOT debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.

4.33.4 Gestión de información de autenticación secreta de usuarios

La SOT se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal.

4.33.5 Verificación de los derechos de acceso de los usuarios

Los propietarios de los activos deben verificar los derechos de acceso de los usuarios a intervalos regulares.

4.33.6 Retiro o reajuste de los derechos de acceso

En la SOT los derechos de acceso a todos los funcionarios y terceros a la información e instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo, o ajuste luego de un cambio de funciones.

4.34 Responsabilidades de los Usuario

Los usuarios son los responsables de salvaguardar la autenticación de su información.

4.34.1 Uso de información secreta de autenticación

En la SOT se debe solicitar a los usuarios seguir las prácticas de la Institución sobre el uso de la información secreta de autenticación.

4.35 Control de Accesos a Sistemas y Aplicaciones

La SOT se debe evitar el acceso no autorizado a los sistemas y aplicaciones.

4.35.1 Restricción del acceso a la información

En la SOT se debe restringir el acceso a la información y a las funciones de aplicación de sistemas de acuerdo a la Política de Gestión de Accesos.

4.35.2 Procedimiento seguro de logeo

En la SOT se debe controlar el acceso a los sistemas y a las aplicaciones, mediante un procedimiento seguro de logeo.

4.35.3 Sistema de gestión de la clave

Los sistemas de gestión de clave deben ser interactivos y asegurar la calidad de las claves en la SOT.

4.35.4 Uso de programas utilitarios privilegiados

En la SOT se debe restringir y controlar el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de la aplicación.

4.35.5 Control de accesos para programar en código fuente

Se debe restringir el acceso al programa de código fuente.

4.36 Criptografía

En la SOT se debe adoptar controles criptográficos en los sistemas de información para el aseguramiento efectivo y protección de la confidencialidad, autenticidad e integridad de la información, mediante la definición y adopción de algoritmos de encriptación apropiados para ser utilizados en los sistemas de información, aplicaciones y plataformas sensibles.

4.36.1 Gestión de las claves

Las llaves criptográficas deben ser protegidas contra pérdida, modificación y destrucción no autorizada a lo largo de todo su ciclo de vida.

4.37 Seguridad física y medioambiental

En la SOT se debe evitar el acceso físico no autorizado, daño e interferencia a la información e instalaciones de procesamiento de la información de la Institución.

4.37.1 Perímetros de Seguridad

En la SOT se deben adoptar perímetros de seguridad adecuados que garanticen el ingreso del personal autorizado a las áreas que procesan información de la Institución, y a áreas que contienen información sensible y crítica, con el fin de evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones.

4.37.2 Controles físicos de los ingresos

En la SOT se deben proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso únicamente del personal autorizado.

4.37.3 Seguridad en las oficinas, salas e instalaciones

En la SOT se deben diseñar y aplicar mecanismos de seguridad físicos en salas, oficinas e instalaciones.

4.37.4 Protección contra las amenazas externas y medioambientales

Los equipos de la SOT deben ser ubicados y protegidos contra amenazas, peligros del medio ambiente, y de las oportunidades de acceso no autorizado, para lo cual se deben aplicar mecanismos de control contra desastres naturales, ataques maliciosos o accidentes para resguardar la seguridad e integridad física de las personas, centros de datos, activos, e instalaciones de la Institución.

4.37.5 Trabajo en áreas seguras

En la SOT se deben diseñar procedimientos para el trabajo en áreas seguras.

4.37.6 Distribución de las zonas de carga

En la SOT los puntos de acceso, tales como las zonas de distribución y carga, y otros puntos por los que podría ingresar personal no autorizado a las instalaciones deben ser controlados, y en la medida de lo posible ser alejados de las instalaciones de procesamiento de información de la Institución, a fin de evitar el acceso no autorizado.

4.38 Equipos

La SOT debe evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la Institución.

4.38.1 Ubicación y protección de los equipos

Los equipos de la SOT deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultados de amenazas y los peligros del medioambiente, así como oportunidades de accesos no autorizados.

4.38.2 Servicio público de soporte

Los equipos de la SOT deben ser protegidos contra fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.

4.38.3 Seguridad en el cableado

En la SOT se debe proteger de cualquier interferencia, interceptación o daño al cableado de energía o telecomunicaciones que transfieren datos o que sirven de apoyo en los servicios de información.

4.38.4 Mantenimiento de los equipos

En la SOT se debe efectuar el mantenimiento de los equipos a fin de garantizar su disponibilidad e integridad continuas.

4.38.5 Retiro de los activos

Los equipos, información o software de la SOT no pueden ser retirados de su lugar sin una previa autorización.

4.38.6 Seguridad de los equipos y bienes fuera de las instalaciones

En la SOT se deben aplicar medidas de seguridad para los activos utilizados fuera de las instalaciones, considerando los diferentes riesgos de trabajar fuera de las instalaciones de la Institución.

4.38.7 Disposición o re-uso seguro de los equipos

Todos los equipos de la SOT que deban ser dados de baja o reasignados deben ser previamente revisados para garantizar que se haya extraído o sobre escrito la información sensible, al igual que las licencias de software antes de ser desechadas o reutilizadas.

4.38.8 Usuarios de equipos abandonados

En la SOT los funcionarios deben garantizar una adecuada protección a los equipos abandonados.

4.38.9 Escritorios y pantallas limpias

En la SOT se debe adoptar la Política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como pantalla limpia en las instalaciones de procesamiento de la información.

4.39 Seguridad de las operaciones

Las operaciones de los recursos TI y de los sistemas de información son esenciales para mantener un alto nivel de servicio. Por lo tanto, se deben desarrollar e implementar medidas de seguridad para mantener el control adecuado sobre las mismas contra pérdidas de información, malware, explotación de vulnerabilidades, entre otros riesgos y amenazas, implementando mecanismos de control para la detección, prevención y recuperación, para la protección de la información, y evitando los accesos a sitios web no autorizados.

4.39.1 Documentación de los procedimientos operacionales

En la SOT se deben documentar los procesos operacionales y ser puestos a disposición de los usuarios autorizados que lo necesiten.

4.39.2 Cambios en la Gerencia

En la SOT se debe mantener un control sobre los cambios en la Institución, y los sistemas que afectan la Seguridad de la Información.

4.39.3 Gestión de la capacidad

En la SOT se debe monitorear y mejorar el uso de los recursos, así como las proyecciones realizadas sobre los requisitos de capacidad futuros para garantizar el desempeño de los sistemas de la Institución.

4.39.4 Separación de ambientes de desarrollo, prueba y de operaciones

Separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de los ambientes de operación.

4.40 Protección contra el malware (programas maliciosos)

La SOT debe garantizar que la información y las instalaciones de procesamiento de la información estén protegidas contra malware.

4.40.1 Controles contra el malware

En la SOT se deben implementar mecanismos de control para la detección, prevención y recuperación, a fin de proteger la información contra el malware, junto con planes de concientización adecuados a los usuarios.

4.41 Backups

Proteger la información, software e imágenes contra los riesgos de daño y pérdida empleando backups de información, los cuales deben ser probados de manera regular, así como los eventos de inicio de sesión que registren las actividades, excepciones, faltas y cualquier evento de Seguridad de la Información.

4.42 Logeo y Monitoreo

En la SOT se deben registrar eventos y generar evidencias.

4.42.1 Eventos de logeo

Se debe llevar a cabo y verificar regularmente eventos de logeo que registren actividades, excepciones, faltas y cualquier evento de Seguridad de la Información.

4.42.2 Protección de la Información de logeo

En la SOT se debe proteger contra la falsificación y accesos no autorizados a los medios de logeo y a la información de logeo.

4.42.3 Logeo del administrador y operador

Los registros de logeo de administradores y operadores en la Institución deben ser protegidos y revisados de manera regular.

4.42.4 Sincronización de los relojes

Se debe sincronizar a una sola fuente de tiempo de referencia los relojes de todos los sistemas de procesamiento de la información correspondientes dentro de SOT.

4.43 Control del Software Operacional

En la SOT se debe garantizar la integridad de los sistemas operacionales.

4.43.1 Instalación de software en los sistemas operacionales

En la SOT se deben implementar procedimientos para controlar la instalación del software en los sistemas operacionales.

4.44 Gestión de Vulnerabilidades Técnicas

Evitar la explotación de las vulnerabilidades técnicas en la Institución.

4.44.1 Gestión de las vulnerabilidades técnicas

Obtener de manera oportuna información sobre las vulnerabilidades técnicas de los sistemas de información utilizados o ser utilizados, evaluando la exposición de la SOT a las vulnerabilidades y tomar medidas adecuadas para el manejo de los riesgos asociados, para lo cual se deben planificar los requisitos y actividades de auditoría que involucren la verificación de los sistemas operacionales; y minimizar las alteraciones a los procesos del negocio.

4.44.2 Restricción en la instalación de software

En la SOT se debe establecer e implementar las reglas que gobiernen la instalación de software.

4.45 Consideraciones de las auditorías sobre los sistemas de información

Se debe minimizar el impacto de las actividades de las auditorías en los sistemas operacionales de la SOT.

4.45.1 Controles de la auditoría sobre los sistemas de información

En la SOT se debe planificar cuidadosamente los requisitos y actividades de la auditoría que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio.

4.46 Seguridad de las comunicaciones

Garantizar la protección de la información en las redes e instalaciones de procesamiento de la información dentro de la SOT y con cualquier entidad externa.

4.46.1 Controles en las redes

Se debe administrar y controlar las redes de la SOT para proteger la información alojada en los sistemas y aplicaciones.

4.46.2 Seguridad de los servicios de las redes

En la SOT se deben identificar los mecanismos de seguridad, los niveles de servicio y requisitos de todos los servicios de redes, a fin de incluirlos en los acuerdos de servicios de redes.

4.46.3 Segregación en las redes

En la SOT se deben segregar grupos de servicios de información, usuarios y sistemas de información.

4.47 Transferencia de la Información

Se debe mantener la Seguridad de la Información transferida dentro de la SOT y con cualquier entidad y desarrollar e implementar mecanismos y medidas de seguridad para el control de las comunicaciones, así como control del cumplimiento de los niveles de servicio y cumplimiento de los acuerdos de confidencialidad sobre la transferencia segura de la información con terceros.

4.47.1 Acuerdos sobre la transferencia de la información

Los acuerdos mantenidos entre la SOT y terceros deben señalar la transferencia segura de la información del negocio.

4.47.2 Mensajes electrónicos

En la SOT se debe proteger adecuadamente la información enviada mediante mensajes electrónicos.

4.47.3 Confidencialidad o acuerdos de no divulgación

Al interior de SOT se debe revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos de no divulgación que reflejan las necesidades de la Institución sobre la protección de la información.

4.48 Adquisición, desarrollo y mantenimiento del sistema

Garantizar que la Seguridad de la Información forme parte integral de los sistemas de información a lo largo de todo su ciclo de vida, incluyendo todas las fases de diseño, desarrollo, mantención, operación y explotación; y garantizar la protección de los datos de prueba utilizados.

4.48.1 Análisis y especificaciones de los requisitos de la Seguridad de la Información

Se debe incluir la Seguridad de la Información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas existentes en SOT.

4.48.2 Seguridad de los servicios de aplicación en las redes públicas

En debe proteger la información de la SOT que pasa a través de las redes públicas de las actividades fraudulentas, controversias, contractuales, divulgación y modificaciones no autorizadas.

4.48.3 Protección de las transacciones de los servicios de aplicación

Se debe proteger la información que provenga de las transacciones de los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicación o reproducción no autorizada de mensajes.

4.49 Seguridad en los procesos del programa de desarrollo y soporte

La SOT debe garantizar que se diseñe e implemente la Seguridad de la Información dentro del ciclo del programa de desarrollo de los sistemas de información, aplicando reglas de desarrollo de software y sistemas a los programas de desarrollo dentro de la Institución.

4.49.1 Procedimiento de control de los cambios de sistemas

Se debe controlar los cambios dentro del ciclo de vida de los programas desarrollados, mediante el uso de procedimientos formales de control de cambios.

4.49.2 Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional

Luego de efectuarse cambios en las plataformas operacionales, se debe revisar y verificar las aplicaciones críticas del negocio a fin de garantizar que no haya un impacto adverso sobre las operaciones o la seguridad organizacional.

4.49.3 Restricción a los cambios de los paquetes de software

No se debe facilitar la modificación de los paquetes de sistemas, puesto que se deben ser limitados a cambios estrictamente necesarios los cuales deben ser controlados.

4.49.4 Principio del sistema de seguridad para la ingeniería

Se debe establecer, documentar, mantener y aplicar los principios de sistemas de seguridad para la ingeniería, a todos los esfuerzos de implementación del sistema.

4.49.5 Ambiente seguro del programa de desarrollo

La SOT debe establecer y proteger adecuadamente los ambientes seguros de desarrollo de los sistemas de desarrollo y la integración de los esfuerzos a lo largo del ciclo de vida del programa de desarrollo del sistema.

4.49.6 Programa de desarrollo subcontratado

La SOT debe supervisar y monitorear las actividades de desarrollo del sistema del ente subcontratado.

4.49.7 Revisión de la seguridad del sistema

En la SOT se deben llevar a cabo revisiones de la funcionalidad de la seguridad durante el desarrollo.

4.49.8 Revisión de la aceptación del sistema

En la SOT se deben establecer programas de verificación de la aceptación y de los criterios relacionados con respecto a los nuevos sistemas de información, renovaciones y nuevas versiones.

4.50 Datos de prueba

En la SOT se debe garantizar la protección de los datos utilizados para la verificación.

4.50.1 Protección de los datos de prueba

Los datos de prueba deben ser seleccionados, protegidos y controlados cuidadosamente.

4.51 Relación con los proveedores

Garantizar la protección de los activos de la información a los que tienen acceso los proveedores, manteniendo un nivel acordado de Seguridad de la Información y de la prestación del servicio alineado a los acuerdos del proveedor, para lo cual se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la SOT.

4.51.1 Consideración de la seguridad en los acuerdos con los proveedores

En la SOT se debe establecer y acordar todos los requisitos relacionados a la Seguridad de la Información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la Institución.

4.51.2 Cadena de suministro de tecnología de la información y comunicación

Los acuerdos con los proveedores deben incluir los requisitos para el manejo de los riesgos de Seguridad de la Información relacionados a los servicios de tecnología de la información y a la comunicación y cadena de suministro de productos.

4.52 Gestión de la prestación del servicio por parte del proveedor

La SOT debe mantener un nivel acordado de Seguridad de la Información y prestación de servicios alineados a los acuerdos del proveedor.

4.52.1 Monitoreo y revisión del servicio de los proveedores

La SOT debe monitorear, revisar y auditar regularmente la prestación de servicios del proveedor.

4.52.2 Cambios en la gestión de servicios de los proveedores

En la SOT se debe gestionar los cambios a las provisiones de los servicios prestados por los proveedores, incluyendo el mantenimiento y mejora de Políticas, procedimientos y controles de Seguridad de la Información, considerando la sensibilidad de la información del negocio, sistemas y procesos involucrados, así como re-evaluación de los riesgos.

4.53 Gestión de los incidentes de Seguridad de la Información

Reportar los eventos de Seguridad de la Información a través de canales establecidos al área de Seguridad de la Información y jefatura inmediata, para evaluación y ejecución de acciones consistentes y efectivas en gestión de los incidentes de Seguridad de la Información que permitirán valorar y comunicar los eventos y debilidades de la seguridad, para lo cual la SOT debe garantizar una aproximación consistente y efectiva a la gestión de los incidentes de Seguridad de la Información, incluyendo la comunicación sobre los eventos y debilidades de la seguridad.

4.53.1 Responsabilidades y procedimientos

La SOT debe establecer responsabilidades de las Gerencias y procedimientos para garantizar una respuesta rápida y adecuada a los incidentes de Seguridad de la Información.

4.53.2 Reporte de los eventos de Seguridad de la Información

En la SOT se debe reportar los eventos de Seguridad de la Información a través de canales adecuados de manera inmediata.

4.52.3 Reporte de las debilidades de la Seguridad de la Información

En la SOT se debe instar a los funcionarios y contratistas que hagan uso de los sistemas de información de la Institución, a tomar nota e informar cualquier debilidad que sea observada o que se sospeche con respecto a los sistemas o servicios.

4.52.4 Evaluación y decisión sobre los eventos de Seguridad de la Información

Se debe evaluar los eventos de seguridad de la Institución y tomar decisiones si deben ser clasificados como incidentes de Seguridad de la Información.

4.52.5 Respuesta a los incidentes de Seguridad de la Información

Se debe responder a los incidentes de Seguridad de la Información acorde los procedimientos documentados.

4.52.6 Aprendizaje de los incidentes de Seguridad de la Información

Se debe usar el conocimiento obtenido del análisis y resolución de los incidentes de la Seguridad de la Información, con la finalidad de reducir la probabilidad o impactos de futuros incidentes.

4.52.7 Recolección de evidencia

La SOT debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información que puede servir como evidencia.

4.53 Gestión de los aspectos de la Seguridad de la Información para la Continuidad del Negocio

La Continuidad de la Seguridad de la Información debe estar inmersa en el Sistema de Gestión de Continuidad del Negocio (SGCN) y Planes de Recuperación de Desastres (DRP) de SOT, a fin de garantizar la disponibilidad de las instalaciones de procesamiento de la información para la recuperación ante cualquier interrupción del negocio sin importar la causa.

4.53.1 Continuidad de los planes de Seguridad de la Información

La SOT debe determinar sus requisitos para la Seguridad de la Información y para la Continuidad de la Gestión de Seguridad de la Información en situaciones adversas, crisis o desastres.

4.53.2 Implementación de la Continuidad de la Seguridad de la Información

La SOT debe establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de la Seguridad de la Información durante una situación adversa.

4.53.3 Verificación, revisión y evaluación de la Continuidad de la Seguridad de la Información

La SOT debe verificar los controles establecidos e implementados para la Continuidad de la Seguridad de la Información, a intervalos regulares con la finalidad de asegurar su validez y efectividad durante situaciones adversas.

4.54 Redundancias

Se debe garantizar la disponibilidad de las instalaciones de procesamiento de la información de la SOT.

4.54.1 Disponibilidad de las instalaciones de procesamiento de la información

En la SOT se debe implementar instalaciones de procesamiento de la información con capacidad adicional y suficiente para cumplir con los requisitos de disponibilidad.

4.55 Cumplimiento

Evitar el incumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas a la Seguridad de la Información y a cualquier requisito de seguridad, con el fin de garantizar que la Seguridad de la Información sea implementada y operada de acuerdo a las Leyes vigentes en el país, así como Políticas y procedimientos establecidos en la SOT.

4.55.1 Identificación de la Ley aplicable y de los requisitos contractuales

La SOT debe identificar de manera explícita, documentar y mantener actualizados todos los requisitos legislativos regulatorios y contractuales, así como el enfoque de la Institución para cumplir con estos requisitos, con respecto a cada sistema de información y a la Institución.

4.55.2 Derechos de propiedad intelectual

En la SOT se deben implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos registrados de software.

4.55.3 Protección de los registros

Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, accesos no autorizados de acuerdo a los requisitos legales, regulatorios, contractuales y de la SOT.

4.55.4 Privacidad y protección de la información que permite identificar a las personas

En la SOT se debe garantizar la privacidad y protección de la información que permita identificar a las personas de acuerdo a lo requerido en la legislación y las regulaciones pertinentes, si fuera aplicable.

4.55.5 Regulación de los controles criptográficos

En la SOT se debe hacer uso de los controles criptográficos en cumplimiento con los acuerdos, leyes y regulaciones correspondientes.

4.56 Revisiones de la Seguridad de la Información

En la SOT se debe garantizar que la Seguridad de la Información sea implementada y operada acorde las Políticas y procedimientos organizacionales.

4.56.1 Revisión independiente de la Seguridad de la Información

Se debe revisar a intervalos planificados o cuando ocurra algún cambio significativo, el enfoque de la Institución para gestionar la Seguridad de la Información y su implementación tales como objetivos, controles, Políticas, procesos y procedimientos.

4.56.2 Cumplimiento de las Políticas y Normas de Seguridad de la Información

En la SOT los Gerentes deben revisar regularmente el cumplimiento de los procedimientos y de procesamiento de la información dentro de su área de responsabilidad, acorde las Políticas, Normas de Seguridad adecuadas y otros requisitos de seguridad.

4.56.3 Revisión del cumplimiento técnico

Los sistemas de información de la SOT deben ser revisados regularmente con respecto al cumplimiento de las Políticas y Normas de Seguridad de la Información de la Institución.

5. FUNCIONES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) ACOGIENDO LA NORMA ISO/IEC 27001:2013

5.1 Comité de Seguridad de la Información

Debe considerar las siguientes responsabilidades:

5.1.1 Políticas, Estándares y Procedimientos

- Validar y aprobar el alcance y límites del SGSI, institución, ubicación, activos y tecnología.
- Validar y autorizar la implementación y operación del SGSI.
- Aprobar las Políticas para el SGSI.
- Aprobar las funciones y responsabilidades en Seguridad de la Información.
- Definir y aprobar la publicación de las normas generales de Seguridad de la Información para empleo y compromiso de todos los colaboradores internos y externos de la Institución.
- Definir oportunidades de mejora y las necesidades de cambios del SGSI.
- Validar y aprobar la gestión de nuevos recursos para establecer, implementar, operar, efectuar seguimientos, revisar, mantener y mejorar continuamente el SGSI.
- Revisar y aprobar la Declaración de Aplicabilidad de Controles propuesta para el SGSI.

5.1.2 Identificación, análisis, valoración, evaluación y tratamiento de riesgos

- Validar y aprobar la metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de Seguridad de la Información identificados en la SOT.
- Validar los niveles de riesgos residuales presentados por el Líder de Seguridad de la Información y Continuidad del Negocio.
- Definir los criterios para la aceptación de riesgos, y los niveles de riesgo aceptables.
- Decidir sobre cualquier decisión o acción relacionada con la actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Validar y aprobar un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de Seguridad de la Información.
- Aprobar y revisar periódicamente las Políticas y Normas de Seguridad de la Información.

5.1.3 Planeación estratégica de la Seguridad de la Información

- Revisar y aprobar la estrategia de Seguridad de la Información de la Institución, con iniciativas tácticas y proyectos que soporten los objetivos de negocio definidos, siempre y cuando se relacionen con la Seguridad de la Información.

- Asegurar que los objetivos de protección de la información sean consistentes con los planes estratégicos de la Institución.
- Revisar y aprobar los indicadores del SGSI.
- Revisar y aprobar los planes de seguridad desarrollados.
- Conocer los planes y estrategias de crecimiento de la SOT, y crecimiento de la infraestructura tecnológica.
- Autorizar la emisión de comunicaciones en la SOT que se refieran a la importancia de cumplir los objetivos de Seguridad de la Información de conformidad con la Política de Seguridad de la Información, responsabilidades y necesidades sobre la mejora continua.
- Actuar como patrocinador en proyectos de Seguridad de la Información que requieran de soporte externo.

5.1.4 Revisión y medición del SGSI

- Conocer los procedimientos de seguimiento y revisión del SGSI.
- Conocer los resultados de las evaluaciones a las vulnerabilidades, amenazas e investigaciones de los incidentes de Seguridad de la Información.
- Conocer los resultados de las revisiones de eficacia del SGSI incluyendo el cumplimiento de la Política, objetivos y revisión de los controles de seguridad, considerando los resultados de las auditorías de seguridad, incidentes, sugerencias y retroalimentación de las partes interesadas.
- Revisar la validez y consistencia del SGSI para asegurar su continuidad, idoneidad y efectividad, a fin de evaluar las necesidades, resultados del seguimiento a la normativa y/o principales incidentes ocurridos en relación con la Seguridad de la Información.

5.1.5 Auditoría

- Conocer y revisar los resultados de las auditorías efectuadas al SGSI en las que se incluya el cumplimiento de la Política, objetivos y revisión de los controles de seguridad, considerando los resultados de las auditorías de seguridad, incidentes, sugerencias y retroalimentación de las partes interesadas.

5.1.6 Gestión de vulnerabilidades

- Aprobar el procedimiento de gestión de vulnerabilidades.
- Gestionar la asignación de los recursos para el análisis de vulnerabilidades sobre la plataforma tecnológica.
- Gestionar la asignación de recursos para ejecutar planes de remediación de las vulnerabilidades.
- Gestionar la asignación de los recursos para el diseño de líneas base de seguridad sobre la plataforma tecnológica.

5.1.7 Manejo de acciones preventivas y correctivas

- Conocer las acciones desarrolladas por las áreas de la SOT para la remediación de las no conformidades u observaciones resultantes de las auditorías.

5.1.8 Gestión de la arquitectura de seguridad

- Analizar y verificar que la arquitectura de seguridad esté alineada con la planeación estratégica de la Institución.
- Gestionar la asignación de los recursos para la compra de soluciones o dispositivos requeridos para la implementación de la arquitectura de seguridad.

5.2 Líder de Seguridad de la Información y Continuidad del Negocio

Representante del SGSI y responsable de participar en las decisiones estratégicas del Comité de Seguridad de la Información. Permite la integración entre los aspectos estratégicos y tácticos que se presenten en el SGSI.

5.2.1 Políticas, Estándares y Procedimientos

- Validar y proponer al Comité de Seguridad de la Información el alcance y límites del SGSI en términos de las características de la SOT, institución, ubicación, activos y tecnología.
- Validar y proponer al Comité de Seguridad de la Información la Política del SGSI.
- Validar y aprobar la documentación desarrollada por el nivel Operativo del SGSI.
- Validar y presentar al Comité la Declaración de Aplicabilidad de los Controles del SGSI.
- Recomendar al Comité la revisión periódica de las Políticas, Normas y Estándares de Seguridad de la Información.
- Verificar el debido cumplimiento de la Política de Seguridad de la Información de la SOT.
- Evaluar las iniciativas planteadas para el fortalecimiento del SGSI y presentarlas al Comité de Seguridad de la Información.
- Apoyar al Comité en la definición de las competencias y habilidades requeridas para los cargos que deben asumir los roles establecidos para la Seguridad de la Información.

5.2.2 Identificación, análisis, valoración, evaluación y tratamiento de riesgos

- Validar y presentar al Comité los criterios para aceptación de riesgos, y los niveles de riesgo aceptables.
- Conocer la revisión de las valoraciones de los riesgos a intervalos planificados, y el nivel de riesgo residual y riesgo aceptable definido para la SOT.
- Conocer los resultados de los riesgos realizados en o por las áreas de la SOT, a fin de definir las acciones para la gestión de riesgos, en las que se incluya:

  - Análisis y evaluación de riesgos.
  - Identificación y evaluación de las opciones para el tratamiento de riesgos.
  - Selección de los objetivos de control para el tratamiento de riesgos.
- Validar y presentar al Comité de Seguridad de la Información los riesgos residuales de las áreas de la SOT.
- Validar la implementación del plan de tratamiento de riesgos para lograr los objetivos de control identificados, considerando el financiamiento y asignación de funciones y responsabilidades.
- Validar la implementación de controles seleccionados para cumplir con los objetivos de Seguridad de la Información.
- Dirigir y monitorear la gestión del riesgo de Seguridad de la Información sobre los activos de información.

5.2.3 Planeación estratégica de la seguridad

- Desarrollar la estrategia de Seguridad de la Información para la SOT y presentarla al Comité de Seguridad de la Información, para su implementación.
- Gestionar los lineamientos estratégicos de la Seguridad de la Información con los objetivos de negocio.
- Validar la implementación y operación del SGSI.
- Facilitar y promover el desarrollo de iniciativas sobre la Seguridad de la Información.
- Definir la estrategia de sensibilización, entrenamiento y educación en Seguridad de la Información y apoyar a los Propietarios de la Información en la ejecución de dicha estrategia.
- Conocer y validar la implementación de programas de formación y toma de conciencia relacionados con el SGSI.
- Validar y presentar al Comité de Seguridad de la Información los planes de seguridad desarrollados.
- Validar y aprobar el procedimiento de asignación de responsabilidades definidas en el SGSI.
- Velar por la integración del SGSI con otros sistemas de gestión definidos por la SOT.

5.2.4 Revisión y medición de SGSI

- Gestionar las métricas de seguridad aprobadas por el Comité de Seguridad de la Información, para monitoreo del cumplimiento de la Seguridad de la Información.
- Conocer y aprobar las revisiones regulares al SGSI que incluyan el cumplimiento de la Política y objetivos del SGSI, y revisión de los controles de seguridad, considerando los resultados de las auditorías de seguridad, incidentes, sugerencias y retroalimentación de las partes interesadas.
- Establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente el SGSI.

- Validar y aprobar el procedimiento para definir las acciones de gestión documental desarrolladas por el nivel Operativo.
- Validar la eficacia de los controles o grupos de controles seleccionados por las áreas.
- Conocer la medición de la eficacia de los controles para verificar que cumplen con los requisitos de seguridad.
- Reportar al Comité de Seguridad de la Información los resultados de gestión, los riesgos y necesidades de protección de la información.

5.2.5 Auditoría

- Aprobar la planificación y desarrollo de las auditorías de seguridad al SGSI y conocer los resultados.

5.2.6 Gestión de vulnerabilidades

- Validar y presentar al Comité de Seguridad de la Información el procedimiento de gestión de vulnerabilidades.
- Validar el plan de trabajo presentado por el nivel Operativo para ejecución de las pruebas de vulnerabilidad.
- Solicitar al Comité de Seguridad de la Información los recursos necesarios para el desarrollo de pruebas de vulnerabilidades.
- Comunicar formalmente a la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales, el cronograma y el plan de trabajo para ejecución de las pruebas de vulnerabilidad.
- Solicitar al Comité de Seguridad de la Información los recursos necesarios para el desarrollo de los planes de remediación.

5.2.7 Manejo de acciones preventivas y correctivas

- Validar y presentar al Comité las acciones preventivas y correctivas a ser tomadas para la remediación de las no conformidades u observaciones encontradas en las auditorías de seguridad.
- Verificar que la son conformidades sean subsanadas.

5.2.8 Gestión de la arquitectura de seguridad

- Revisar y validar el diseño de la arquitectura de seguridad desarrollado por el nivel Operativo.
- Solicitar al Comité de Seguridad de la Información los recursos necesarios para la implementación de la arquitectura de seguridad.
- Revisar los planes definidos para la implementación de la arquitectura de seguridad.

- Coordinar con la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales el cronograma y plan de trabajo para la implementación de la arquitectura de seguridad.
- Verificar que el plan de implementación de la arquitectura sea cumplido acorde lo definido.
- Evaluar los posibles cambios que se puedan presentar durante la implantación de la arquitectura de seguridad.

5.2.9 Continuidad del Negocio

- Velar por el desarrollo, establecimiento, actualización y pruebas programadas a los planes de continuidad definidos por la SOT.
- Apoyar a las áreas de la SOT en la definición de sus planes de continuidad.
- Velar por la disponibilidad del Plan de Continuidad del negocio.
- Gestionar la documentación del Plan de Continuidad del negocio.

5.3 Líder de Seguridad de la Información

Encargado de coordinar la ejecución de las directrices de planeación, implementación, revisión y mantenimiento del SGSI emitidas por los niveles Estratégico y Táctico.

5.3.1 Políticas, Estándares y Procedimientos

- Presentar al Líder de Seguridad de la Información y Continuidad del Negocio, la Declaración de Aplicabilidad de Controles para el SGSI.
- Entender las necesidades de Seguridad de la Información para LA SOT a fin de implementar y monitorear las Políticas, normas y procedimientos de seguridad que cubran los objetivos de negocio.
- Medir el nivel de cumplimiento de las Políticas, estándares y procedimientos de Seguridad de la Información en la SOT.
- Garantizar el establecimiento, mejora y actualización del manual del SGSI de la SOT.
- Definir cuáles son los estándares y procedimientos de Seguridad de la Información que deben ser considerados por la SOT para ser presentados al Líder de Seguridad de la Información y Continuidad del Negocio.
- Mantener actualizada la normativa de seguridad y la lista de todos los Propietarios de la Información.

5.3.2 Identificación, análisis, valoración, evaluación y tratamiento de riesgos

- Definir y proponer al Líder de Seguridad de la Información y Continuidad del Negocio la metodología para la identificación, valoración, clasificación y tratamiento de los activos de información.

- Llevar el control del mantenimiento y actualización periódica del inventario de los activos de información.
- Definir y proponer al Líder de Seguridad de la Información y Continuidad del Negocio los criterios y niveles de aceptación del riesgo.
- Coordinar la ejecución de revisiones de valoraciones de los riesgos a intervalos planificados, considerando el nivel de riesgo residual y riesgo aceptable.
- Participar en el proceso de planificación de contingencias, y en las pruebas de implementación de los planes de recuperación ante desastres definidos.
- Coordinar la ejecución de la gestión de riesgos que incluya:
    - Análisis y evaluación de riesgos.
    - Identificación y evaluación de opciones para tratamiento de riesgos.
    - Selección de objetivos de control para el tratamiento de riesgos.
- Recibir de las áreas responsables los riesgos residuales y presentarlos al Líder de Seguridad de la Información y Continuidad del Negocio.
- Consolidar la información sobre el plan de tratamiento de riesgos diseñado por las áreas responsables y presentarlo al Líder de Seguridad de la Información y Continuidad del Negocio.
- Coordinar la implementación del plan de tratamiento de riesgos en cada una de las áreas.
- Coordinar la implementación de controles seleccionados en cada área.
- Dar soporte a la Alta Dirección en los procesos de:
    - Definición de los Propietarios de la Información.
    - Identificación de la información sensible.
    - Identificación de las medidas de seguridad necesarias en cada nuevo sistema de aplicación o desarrollo para cumplir con la normativa.
    - Seguimiento a la implementación de dichas medidas.

5.3.3 Planeación estratégica de la seguridad

- Definir y proponer al Líder de Seguridad de la Información y Continuidad del Negocio el alcance y límites del SGSI en términos de las características de la SOT, institución, ubicación, activos y tecnología.
- Coordinar la implementación y operación del SGSI.
- Implementar en conjunto con la Dirección de Talento Humano, programas de concientización permanente para los colaboradores sobre la Seguridad de la Información y su mantenimiento a futuro.
- Facilitar y promover el desarrollo de iniciativas sobre Seguridad de la Información.
- Garantizar la integración del SGSI con otros sistemas de gestión en la Institución.

5.3.4 Revisión y medición del SGSI

- Coordinar la definición para la eficacia de los controles o grupos de controles seleccionados por las áreas.
- Coordinar y participar en el diseño de la implementación de programas de

formación y toma de conciencia relacionados con el SGSI.

- Validar la necesidad de nuevos recursos para el SGSI para establecer, implementar, revisar, mantener y mejorar el SGSI y presentarla al Líder de Seguridad de la Información y Continuidad del Negocio.
- Participar en el diseño y definición de los procedimientos y controles para detectar y brindar respuestas oportunas a los incidentes de seguridad.
- Coordinar la ejecución de procedimientos para el seguimiento y revisión del SGSI.
- Coordinar la ejecución de acciones para medir la eficacia de los controles de seguridad implementados.
- Consolidar la información de las áreas sobre los planes de seguridad desarrollados y presentarlos a al Líder de Seguridad de la Información y Continuidad del Negocio.
- Gestionar la documentación del SGSI.
- Coordinar las acciones para el establecimiento, cumplimiento y mantenimiento del SGSI.
- Coordinar y participar en el diseño de procedimientos para la asignación de responsabilidades definidas en el SGSI.
- Coordinar la ejecución de revisiones regulares al SGSI que incluyan el cumplimiento de la Política y objetivos del SGSI, y revisión de los controles de seguridad, considerando los resultados de las auditorías de seguridad, incidentes, sugerencias y retroalimentación de las partes interesadas.
- Liderar la ejecución de análisis e investigaciones sobre los incidentes de Seguridad de la Información.

5.3.5 Auditoría

- Coordinar la ejecución de las auditorías planificadas al SGSI.

5.3.6 Continuidad del Negocio

- Apoyar en los procesos de implementación y actualización de los planes de continuidad.
- Apoyar en la definición de los cronogramas de prueba de los planes de continuidad.
- Apoyar a los procesos en la definición de sus planes de continuidad.
- Velar por el cumplimiento de la Seguridad de la Información, en el desarrollo, implementación, pruebas y actualización de los planes de continuidad.

5.3.7 Gestión de Vulnerabilidades

- Aprobar los planes y cronogramas para la ejecución de las pruebas de vulnerabilidades a la plataforma tecnológica.
- Aprobar los cronogramas y planes para la remediación de las vulnerabilidades encontradas.

- Definir el procedimiento para la gestión de vulnerabilidades.

5.3.8 Manejo de acciones preventivas y correctivas

- Plantear sugerencias de acciones preventivas y/o correctivas para ser desarrolladas por las áreas responsables, y posteriormente validar las acciones propuestas por las áreas.

5.3.9 Gestión de la arquitectura de seguridad

- Realizar el diseño de la arquitectura de seguridad.
- Participar en la investigación y recomendación de productos de seguridad en conjunto con la Dirección de Tecnología e Información, para la implementación de las medidas de seguridad en los sistemas.
- Definir y proponer el plan para la implementación de la arquitectura de seguridad.
- Monitorear el cumplimiento y efectividad de la arquitectura de seguridad.

5.4 Analistas Seguridad de la Información

Responsables de ejecutar todas las acciones definidas y aprobadas por los niveles Estratégico y Táctico.

5.4.1 Políticas, Estándares y Procedimientos

- Efectuar, recibir y validar los escaneos de vulnerabilidades y pruebas de penetración a los sistemas de información.
- Elaborar esquemas de tratamiento para las vulnerabilidades encontradas.
- Reportar al Líder de Seguridad de la Información, las vulnerabilidades detectadas junto con su criticidad y urgencia de atención para su remediación.
- Verificar la eficacia de la remediación de las vulnerabilidades detectadas sobre el software y hardware empleando escaneos de vulnerabilidad y pruebas de penetración.
- Identificar los diferentes elementos probatorios informáticos vinculados a incidente de Seguridad de la Información, procurando determinar la relación directa entre los elementos encontrados y los hechos.
- Recoger, conservar y analizar las pruebas procedentes de un sistema informático comprometido en un incidente de Seguridad de la Información para determinar cambios en el sistema y ayudar a reconstruir los eventos que generaron dicho incidente.
- Presentar y reportar al Líder de Seguridad de la Información los hallazgos encontrados producto del análisis de las evidencias digitales.
- Identificar y evaluar temas técnicos referentes a proyectos e implementaciones de Seguridad de la Información.
- Recibir y analizar los incidentes de Seguridad de la Información con el fin de determinar el alcance del incidente y los niveles de impacto generados por la

materialización del mismo.

- Direccionar los incidentes de Seguridad de la Información hacia los gestores o áreas responsables según el impacto ocasionado.
- Reportar al Líder de Seguridad de la Información, los incidentes de Seguridad de la Información presentados al igual que contramedidas con el fin de evitar la recurrencia.
- Apoyar en la respuesta a los incidentes de Seguridad de la Información mediante asistencia técnica en la interpretación de los datos recopilados y en la orientación de estrategias para la mitigación de riesgos de Seguridad de la Información.
- Desarrollar estrategias de respuesta a incidentes basadas en históricos de incidentes de Seguridad de la Información.
- Monitorear los logs de los equipos críticos con el fin de analizar actividades inusuales y reportarlos al Líder de Seguridad de la Información.
- Diseñar reglas para la correlación de eventos que permitan alertar situaciones anómalas que atenten contra la Confidencialidad, Integridad y Disponibilidad de la información.

5.5 Cláusulas y Objetivos de la Norma ISO/IEC 27001:2013 (ANEXO A)

Es importante considerar que los objetivos y controles de la Norma Internacional ISO/IEC 27001:2013, corresponden a aquellos detallados en la Norma Internacional ISO/IEC 27002:2013, Cláusulas de la 5 a la 18, mismos que son expuestos a continuación:

Anexo A de la Norma Internacional ISO/IEC 27001:2013:

ANEXO A de la Norma ISO 27001:2013 – CLAUSULAS Y CONTROLES
5. POLÍTICAS DE SEGURIDAD Gestión de la Gerencia para la Seguridad de la Información • Política de Seguridad de la Información • Revisión de la Política de Seguridad de la Información
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN Organización Interna • Funciones y responsabilidades de la seguridad de la información • Segregación de funciones • Contacto con las autoridades • Contacto con grupos de interés • Seguridad de la información en la gestión del proyecto Equipos móviles y trabajo a distancia • Política de los equipos móviles • Trabajo a distancia
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS Antes del reclutamiento • Filtración • Términos y condiciones de empleo Durante el trabajo • Responsabilidades de la Gerencia • Concientización, educación y capacitación sobre seguridad de la información • Procesos disciplinarios

ANEXO A de la Norma ISO 27001:2013 – CLAUSULAS Y CONTROLES
Término y cambio de empleo • Término o cambio de responsabilidades de empleo
8. GESTIÓN DE ACTIVOS Responsabilidad sobre los Activos • Inventario de Activos • Propiedad de los activos • Uso aceptable de los activos • Retorno de los activos Clasificación de la Información • Clasificación de la información • Etiquetada de la información • Manejo de los activos Manejo de los medios de comunicación • Gestión de medios de comunicación removibles • Disposición de los medios de comunicación • Transferencia física de los medios de comunicación
9. CONTROL DE ACCESOS Control de Acceso • Política de control de acceso • Acceso a las redes y a los servicios de las redes Gestión del Acceso al Usuario • Registro y des-registro del usuario • Provisión de acceso al usuario • Gestión de los derechos de acceso privilegiado • Gestión de información de autenticación secreta de usuarios • Retiro o ajuste de los derechos de acceso Responsabilidades del usuario • Uso de información secreta de autenticación Control de acceso a sistemas y aplicaciones • Restricción del acceso a la información • Procedimiento seguro de logeo • Sistema de gestión de la clave • Uso de programas utilitarios de privilegio • Control del acceso para programar el código fuente
10. CIFRADO Critografía • Política del uso de controles criptográficos • Gestión de las claves
11. SEGURIDAD FÍSICA Y AMBIENTAL Seguridad física y ambiental • Perímetro de seguridad física • Controles físicos de los ingresos • Seguridad de las oficinas salas e instalaciones • Protección contra las amenazas externas y medioambientales • Trabajo en áreas seguras • Distribución de las zonas de carga Equipos • Ubicación y protección de los equipos • Servicios públicos de soporte • Seguridad en el cableado • Mantenimiento de los equipos • Retiro de los activos

ANEXO A de la Norma ISO 27001:2013 – CLAUSULAS Y CONTROLES
• Seguridad de los equipos y bienes fuera de las instalaciones • Disposición o re-uso seguro de los equipos • Usuario de equipo abandonado • Política de escritorio y pantallas limpias
12. SEGURIDAD EN LA OPERATIVA Seguridad de las Operaciones • Documentación de los procedimientos operacionales • Cambios en la gerencia • Gestión de la capacidad • Separación de ambientes de desarrollo, prueba y de operaciones Protección contra el malware (programa malicioso) • Controles contra el malware Backup • Backup de la información Logeo y Monitoreo • Eventos de logeo • Protecciói n de la información del logeo • Logeo del administrador y operador • Sincronización de los relojes Control de software operacional • Instalación del software en los sistemas operacionales Gestión de vulnerabilidades técnicas • Gestión de vulnerabilidades técnicas • Restricción en la instalación de software Consideraciones de las auditorías sobre los sistemas de información • Controles de la auditoría sobre los sistemas de información
13. SEGURIDAD EN LAS TELECOMUNICACIONES Gestión de la seguridad en las redes • Control en las redes • Seguridad de los servicios de las redes • Segregación en las redes Transferencia de la información • Políticas y procedimientos de la transferencia de la información • Acuerdos sobre la transferencia de la información • Mensajes electrónicos • Confidencialidad o acuerdos no divulgados
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS Requisitos de seguridad de los sistemas de información • Análisis y especificaciones de los requisitos de la seguridad de la información • Seguridad de los servicios de aplicación en las redes públicas • Protección de las transacciones de los servicios de aplicación Seguridad en los procesos del programa de desarrollo y software • Política del programa de desarrollo seguro • Procedimiento de control de los cambios de sistema • Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional • Restricción a los cambios de los paquetes de software • Principios del sistema de seguridad para la ingeniería • Ambiente seguro del programa del desarrollo • Programa de desarrollo subcontratado • Revisión de la seguridad del sistema • Revisión de la aceptación del sistema Datos de prueba

ANEXO A de la Norma ISO 27001:2013 – CLAUSULAS Y CONTROLES
• Protección de los datos de prueba
15. RELACIONES CON SUMINISTRADORES Seguridad de la información en las relaciones con los proveedores • Política de seguridad de la información sobre las relaciones con los proveedores • Consideración de la seguridad en los acuerdos con los proveedores • Cadena de suministros de tecnología de la información y comunicación Gestión de la prestación del servicio por parte del proveedor • Monitoreo y revisión del servicio de los proveedores • Cambios en la gestión del servicio de los proveedores
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Gestión de los incidentes de la seguridad de la información • Responsabilidades y procedimientos • Reporte de los eventos de seguridad de la información • Reporte de la debilidad de la seguridad de la información • Evaluación y decisión sobre los eventos de seguridad de la información • Respuestas a los incidentes de seguridad de la información • Aprendizaje de los incidentes de seguridad de la información • Recolección de evidencias
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO Continuidad de la seguridad de la información • Continuidad de los planes de seguridad de la información • Implementación de la continuidad de la seguridad de la información • Verificación, revisión y evaluación de la continuidad de la seguridad de la información Redundancias • Disponibilidad de instalaciones de procesamiento de la información
18. CUMPLIMIENTO Cumplimiento de los requisitos legales y contractuales • Identificación de la ley aplicable y de los requisitos contractuales • Derechos de la propiedad intelectual • Privacidad y protección de la información que permite identificar a las personas • Regulación de los controles criptográficos Revisiones de la seguridad de la información • Revisión independiente de la seguridad de la información • Cumplimiento de las políticas y normas de seguridad de la información • Revisión del cumplimiento técnico

Tabla: Cláusulas y Controles Anexo A de la Norma Internacional ISO/IEC 27001:2013 para análisis de brecha de la Seguridad de la Información.

Fin del documento.

Atentamente,

Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales

Mgs. Mónica Liyana García
COORDINADORA GENERAL DE DESARROLLO DE SOFTWARE E INFRAESTRUCTURA DE DATOS GEOESPACIALES - CGDIG