## ANEXO A

# Requerimientos básicos en la gestión de la seguridad de la información

Los siguientes requerimientos, son los considerados básicos para la gestión de la seguridad de la información al momento de iniciar las operaciones como Operador de Servicios Electrónicos, por lo que deben ser de cumplimiento obligatorio y han sido seleccionados de la Norma Internacional ISO/IEC 27002 – 2013 Code of Practice for Information Security Controls.

La guía de implementación de la referida norma, deberá ser tomada en cuenta de forma imperativa, para el propósito de cumplimiento de estos requerimientos.

**Ámbito/Categoría/Control**

**5. POLÍTICAS DE SEGURIDAD**

**5.1 Dirección de la Gerencia para la seguridad de la información.**
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.

**5.1.1 Políticas para la seguridad de la información.**
Conjunto de políticas para la seguridad de la información que deberán ser definidas y aprobadas por la gerencia, publicadas y comunicadas a los empleados y a las partes externas relevantes.

**5.1.2 Revisión de las políticas de seguridad de la información.**
Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y continua efectividad.

**6. ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION**

**6.1Organización interna.**
Objetivo: establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

**6.1.1 Roles y responsabilidad de seguridad de la información.**
Todos los roles y responsabilidades de seguridad de la información deberán estar definidas y asignados.

**6.1.2 Segregación de deberes o funciones.**
Las funciones y áreas de responsabilidad que pudieran entrar en conflicto, deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional, o por el mal uso de los activos de la organización.

**6.2 Dispositivos móviles y teletrabajo.**
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.

**6.2.1 Política de dispositivos móviles.**
Contar con políticas y medidas de seguridad de soporte que deberán ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.

**7. SEGURIDAD DE LOS RECURSOS HUMANOS**

**7.1 Antes del empleo.**
Objetivo: Asegurar que los empleados y contratistas entienden sus responsabilidades y son competentes para los roles que se les ha asignado.

**7.1.1 Selección.**
Las verificaciones de los antecedentes de todos los candidatos a ser empleados deberán ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, los que deberán ser ~~en~~ un número proporcional a las necesidades del negocio, a la clasificación de la información a la que se tendrán acceso y a los riesgos percibidos.

**7.1.2 Términos y condiciones del empleo.**
Los acuerdos contractuales con los empleados y contratistas deben contemplar las responsabilidades de éstos y de la organización respecto de la seguridad de la información.

**Ámbito/Categoría/Control**

**7.2 Durante el empleo.**

Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.

**7.2.1 Responsabilidad de la Alta Gerencia.**

La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.

**7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información.**

Todos los empleados de la organización, y cuando fuera relevante, los contratistas, deben recibir educación y capacitación sobre la conciencia de la seguridad de la información; así como actualizaciones regulares sobre las políticas y procedimientos de la organización, acorde con la función del trabajo que cumplen.

**7.2.3 Proceso disciplinario.**

Se deberá contar con un proceso disciplinario formal y comunicarlo, para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.

**7.3 Terminación y cambio de empleo.**

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

**7.3.1 Terminación o cambio de responsabilidades del empleo.**

Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo, deberán ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.

**8. GESTIÓN DE ACTIVOS**

**8.3 Manejo de los medios de almacenamiento.**

Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en medios.

**8.3.2 Disposición de medios.**

La información y sus medios de almacenamiento deberán eliminarse mediante procedimientos formales, cuando ya no se requieran.

**9. CONTROL DE ACCESOS**

**9.1 Requisitos de la empresa para el control de accesos.**

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

**9.1.1 Política de control de accesos.**

Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de la seguridad de la información.

**9.2 Gestión de acceso de usuario.**

Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.

**9.2.1 Registro y baja de usuarios.**

Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.

**9.2.2 Aprovisionamiento de acceso a usuarios.**

Un proceso formal de aprovisionamiento de acceso a usuarios deberá ser implementado para asignar o revocar los derechos de acceso, de todos los tipos de usuarios para todos los sistemas y servicios.

**9.2.3 Gestión de los derechos de acceso privilegiados.**

La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.

**9.2.5 Revisión de derechos de acceso de usuarios.**

Los propietarios de los activos deben revisar los derechos de acceso de usuarios en intervalos regulares de tiempo.

**9.4 Control de acceso a sistemas y aplicaciones.**

Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

**9.4.1 Restricción del acceso a la información.**

El acceso a la información y a las funciones del sistema de aplicación debe ser restringido, en concordancia con la política de control de acceso.

**9.4.3 Sistema de Gestión de contraseñas.**

| Ámbito/Categoría/Control |
|---|
| Los sistemas de gestión de contraseñas deben ser interactivos y asegurar contraseñas de calidad. |
| **9.4.5 Control de acceso al código fuente de los programas.**<br>El acceso al código fuente de los programas debe ser restringido |
| **10. CRIPTOGRAFIA** |
| **10.1 Controles criptográficos.**<br>Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información. |
| **10.1.1 Política de uso de los controles criptográficos.**<br>Contar con una política sobre el uso de controles criptográficos para la protección de la información |
| **10.1.2 Gestión de claves.**<br>Contar con una política sobre el uso, protección y tiempo de vida de las claves criptográficas a través de todo su ciclo de vida. |
| **11. SEGURIDAD FÍSICA Y AMBIENTAL** |
| **11.1 Áreas seguras.**<br>Objetivo: Impedir el acceso físico no autorizado, daño e interferencia a la información, así como a las instalaciones donde ésta es procesada. |
| **11.1.1 Perímetro de seguridad física.**<br>Los perímetros de seguridad deben ser definidos y utilizados para proteger a las áreas que contienen información crítica o sensible y a las instalaciones donde se procesa dicha información. |
| **11.1.2 Controles físicos de entrada.**<br>Las áreas seguras deben estar protegidas por medio de controles apropiados de ingreso, para asegurar que solo personal autorizado puede ingresar. |
| **11.1.3 Asegurar áreas, oficinas e instalaciones.**<br>Se deberá diseñar e implementar mecanismos de seguridad en las oficinas, áreas e instalaciones, donde se almacena o se procesa la información. |
| **11.1.4 Protección contra las amenazas externas y ambientales.**<br>Se deberá diseñar e implementar mecanismos de protección física contra desastres naturales, ataques maliciosos o accidentes |
| **11.2 Equipamiento.**<br>Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización. |
| **11.2.7 Disposición (eliminación) o reutilización segura de equipos.**<br>Todos los elementos del equipo que contengan medios de almacenamiento deberán ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura, antes de su puesta a disposición o reutilización |
| **11.2.8 Equipo de usuario desantendido.**<br>Los usuarios deben asegurar que el equipo desatendido tenga la protección apropiada. |
| **11.2.9 Política de escritorio limpio y pantalla limpia.**<br>Se debe adoptar una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información. |

**Ámbito/Categoría/Control**

**12. SEGURIDAD EN LAS OPERACIONES**

**12.1 Procedimientos Operacionales y Responsabilidades.**
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.

**12.1.1 Documentación de procedimientos operacionales.**
Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan.

**12.1.2 Gestión de cambios.**
Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información, deben ser controlados.

**12.1.4 Gestión de la capacidad.**
El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.

**12.1.4 Separación de los ambientes de desarrollo, pruebas y operación.**
Los entornos de desarrollo, pruebas y operaciones deben de estar separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

**12.2 Protección contra código malicioso.**
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.

**12.2.1 Controles contra el código malicioso.**
Se deberá implementar controles de detección, prevención y recuperación para proteger la información contra códigos maliciosos, en combinación con una concientización apropiada a de los usuarios.

**12.3 Respaldo.**
Objetivo: Proteger contra la pérdida de datos.

**12.3.1 Respaldo de la información.**
Se deberán realizar copias de respaldo de la información, del software y de las imágenes del sistema y probadas regularmente, en concordancia con una política de respaldo definida.

**12.4 Registros y monitoreo.**
Objetivo: Registrar eventos y generar evidencia.

**12.4.1 Registro de eventos.**
Se deberán producir, mantener y revisar regularmente los registros (logs) de eventos de actividades de usuarios, excepciones, fallas e incidencias de seguridad de la información.

**12.4.4 Sincronización de relojes.**
Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad, deberán estar sincronizados a una fuente de tiempo de referencia única.

**12.7 Consideraciones de auditoría de sistemas de información.**
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

**12.7.1 Controles de auditoría de sistemas de información.**
Los requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción de los procesos del negocio.

**13. SEGURIDAD EN LAS TELECOMUNICACIONES**

**13.1 Gestión de la seguridad en las redes.**
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.

**13.1.1 Controles de red.**
Las redes deberán ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.

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

**13.2.1 Políticas y procedimientos de transferencia de información.**
Deberá aplicarse políticas, procedimientos y controles de transferencia formales, para proteger la información a través del uso de todo tipo de instalaciones de comunicación.

| Ámbito/Categoría/Control |
|---|
| **13.2.4 Acuerdos de confidencialidad o no divulgación.**<br>Los requisitos para los acuerdos de confidencialidad o no divulgación, que reflejan las necesidades de la organización para la protección de la información, deberán ser identificados, revisados regularmente y documentados. |
| **14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN** |
| **14.1 Requisitos de seguridad de los sistemas de información.**<br>Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas. |
| **14.1.1 Análisis y especificación de los requisitos de seguridad de la información.**<br>Los requisitos relacionados a la seguridad de la información deberán ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas existentes. |
| **14.1.3 Protección de transacciones en servicios de aplicación.**<br>La información involucrada en las transacciones de los servicios de aplicación debe ser protegida para prevenir la transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes. |
| **14.2 Seguridad en los procesos de desarrollo y soporte.**<br>Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información. |
| **14.2.1 Política de desarrollo seguro de software.**<br>Los desarrollos de software y sistemas dentro de la organización deben contar con reglas establecidas. |
| **14.2.9 Pruebas de aceptación del sistema.**<br>Los nuevos sistemas de información, actualizaciones y nuevas versiones, deben contar con programas de pruebas y criterios de aceptación. |
| **15. RELACIONES CON PROVEEDORES** |
| **15.1 Seguridad de la información con el proveedor.**<br>Objetivo: Asegurar protección a los activos de la organización que son accesibles a los proveedores. |
| **15.1.1 Política de seguridad de la información en las relaciones con el proveedor.**<br>Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben estar acordados con el proveedor y ser documentados. |
| **15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores.**<br>Se debe establecer con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer componentes de infraestructura tecnológica para la información; todos los requisitos relevantes de seguridad de la informacion. |
| **15.2 Gestión de entrega del servicio por proveedores.**<br>Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores. |
| **15.2.1 Monitoreo y revisión de los servicios de los proveedores.**<br>Las organizaciones deberán monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores. |
| **16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN** |
| **16.1 Gestión de incidentes de seguridad de la información y mejoras.**<br>Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación de debilidades y eventos de seguridad. |
| **16.1.1 Responsabilidades y procedimientos.**<br>Se deben establecer responsabilidades de los procedimientos y de la gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. |
| **16.1.2 Reporte de eventos de seguridad de la información.**<br>Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados, tan rápido como sea posible. |
| **16.1.6 Aprendizaje de los incidentes de seguridad de la información.**<br>El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información, deberá ser utilizado para reducir la probabilidad o el impacto de incidentes futuros. |

| Ámbito/Categoría/Control |
|---|
| **16.1.7 Colección de evidencia.**<br>La organización deberá definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. |
| **17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO** |
| **17.1 Continuidad de la seguridad de la información.**<br>Objetivo: La continuidad de seguridad de la información deberá estar embebida en los sistemas de gestión de continuidad del negocio de la organización. |
| **17.1.1 Planificación de continuidad de seguridad de la información.**<br>La organización deberá determinar los requisitos de la seguridad de la información y de la continuidad de su gestión en situaciones adversas, por ejemplo durante una crisis o desastre. |
| **17.1.2 Implementación de continuidad de seguridad de la información.**<br>La organización deberá establecer, documentar, implementar y mantener los procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa. |
| **17.1.3 Verificación, revisión y evaluación de continuidad de seguridad de la información.**<br>La organización deberá verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares, para asegurarse que son válidos y efectivos durante situaciones adversas. |
| **18. CUMPLIMIENTO.** |
| **18.1 Cumplimiento con requisitos legales y contractuales.**<br>Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad. |
| **18.1.1 Identificación de requisitos contractuales y de legislación aplicable.**<br>Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos, deben estar explícitamente identificados, documentados y actualizados, para cada sistema de información y para la organización. |
| **18.1.3 Protección de registros.**<br>Los registros deberán estar protegidos ante cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio. |
| **18.2 Revisiones de la seguridad de la información.**<br>Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos. |
| **18.2.1 Revisión independiente de la seguridad de la información.**<br>El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) deberá ser revisado independientemente a intervalos planeados, o cuando ocurran cambios significativos. |
| **18.2.2 Cumplimiento de políticas y estándares de seguridad.**<br>Los gerentes deberán revisar regularmente el cumplimiento de políticas, normas y otros requisitos de seguridad, dentro del ámbito de su competencia. |
| **18.2.3 Revisión del cumplimiento técnico.**<br>Los sistemas de información deberán ser revisados regularmente, con la finalidad de asegurar el cumplimiento de las políticas y normas de seguridad de la información de la organización. |

**Aspectos complementarios para la implementación:**

1. Los términos a utilizar en todo lo relacionado a la materia de la seguridad de la información, son los establecidos en la norma internacional ISO/IEC 27000:2016 Overview and vocabulary y en el SC 27 Standing Document 6 (SD6): Glossary of IT Security Terminology.

2. Los procesos de desarrollo de ingeniería de sistemas y de ingeniería de software deben cumplir con lo establecido por las normas internacionales ISO/IEC 15288 e ISO/IEC 12207, respectivamente.

3. Se debe implementar una política criptográfica que cumpla con los intereses, regulaciones y restricciones del ordenamiento jurídico nacional, de manera tal que salvaguarde aspectos como la confidencialidad de la información, reserva tributaria, entre otros.

4. Se debe establecer controles criptográficos para lograr los diferentes objetivos de seguridad de la información (confidencialidad, integridad/autenticidad, no repudio, autenticación, entre otros) en la solución implementada, dentro de los cuales deben utilizar los equipos de gestión criptográfica HSM. Se debe tomar en consideración el cumplimiento de los estándares siguientes:

    a) En el caso de uso exclusivo del equipo:

    - El estándar FIPS 140-2 Nivel 2
    - El estándar Common Criteria EAL4

    b) En el caso de uso compartido del equipo:

    - El estándar FIPS 140-2 Nivel 3
    - El estándar Common Criteria EAL4

5. Se debe implementar una política y reglas de desarrollo seguro de software y de sistemas, de acuerdo con lo establecido por el protocolo o Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP), para todo el software utilizado en la solución implementada.

6. Llevar un registro de los incidentes presentados respecto de la seguridad de la información, de manera que pueda ser compartido entre los diversos actores del sistema de emisión electrónica, para reducir la probabilidad e impacto de incidentes futuros.

7. Haber realizado las pruebas de intrusión o evaluaciones de vulnerabilidad (Ethical Hacking, entre otros) realizadas dentro del marco de la revisión del cumplimiento técnico de los requerimientos establecidos para la gestión de la seguridad de los sistemas de información.