Seguridad en los Sistemas de Información Disposición ONTI N.º 1/2015

1. Introducción
    - Alcance: gestionar la SI, los sistemas informáticos y el ambiente tecnológico del organismo
    - Define SI y por qué es necesaria
    - Cómo identificar requerimientos de seguridad y cómo evaluar los riesgos
    - Comenzar implementando controles
2. Términos y definiciones
    - Seguridad de la información: confidencialidad, integridad, disponibilidad, autenticidad, auditabilidad, protección a la duplicación, no repudio, legalidad, confiabilidad
    - Evaluación de riesgos: probabilidad e impacto
    - Tratamiento de riesgos
    - Gestión de riesgos: actividades para dirigir y controlar una organización en lo que concierne al riesgo
    - Comité de SI: cuerpo integrado por representantes de todas las áreas sustantivas del organismo, para garantizar el apoyo de las autoridades a la SI
    - Responsable de SI: supervisa el cumplimiento de la política y asesora
    - Incidente de seguridad: evento adverso que compromete o puede comprometer las dimensiones CIA
    - Riesgo, amenaza y vulnerabilidad
    - Control: medio para gestionar el riesgo
3. Estructura de la política modelo
    - Cuatro capítulos introductorios
    - Catorce cláusulas: contienen categorías (grupos de controles), cada una con un objetivo y uno o más controles a realizar

4. Tratamiento de riesgos de seguridad: busca conocer los riesgos a los que se expone el organismo en materia de seguridad de la información. El comité de SI es responsable de que se gestionen los riesgos de SI.

- Evaluación de los riesgos: periódicamente y tras cambios significativos se debe evaluar los riesgos identificándolos, cuantificándolos y priorizándolos en función de criterios de aceptación.
- Tratamiento de riesgos: definir los criterios de aceptación de riesgos, elección del método para tratar cada riesgo: mitigar, transferir, evitar o aceptar.

5. Cláusula: política de seguridad de la información
    - Objetivo
        i. Proteger los recursos de información
        ii. Asegurar la implementación de las medidas de seguridad de la política
        iii. Mantener la política actualizada
    - Categorías
        i. Política de Seguridad de la Información
            a) Objetivo: proporcionar a la Dirección Superior dirección y soporte para la seguridad de la información. Dirección de la política en línea con los objetivos
            b) Controles
                1º Documento de la política de seguridad de la información
                2º Revisión de la política de seguridad de la información
6. Cláusula: organización
    - Objetivo
        i. Administrar la SI y establecer un marco gerencial
        ii. Fomentar la consulta y cooperación con organismos especializados por asesoría en SI
        iii. Aplicación de medidas de seguridad adecuadas en accesos de terceros a la información del organismo
    - Categorías
        i. Organización interna
            a) Objetivo
                1º Manejar la SI dentro del organismo
                2º Establecer un marco gerencial para iniciar y controlar la implementación de la SI
                3º Aprobar la política, asignar los roles y coordinar y revisar la implementación de la SI
            b) Controles
                1º Compromiso de la dirección
                2º Coordinación de la SI
                3º Asignación de responsabilidades
                4º Autorización para Instalaciones de Procesamiento de Información
                5º Acuerdos de confidencialidad
                6º Contacto con otros organismos
                7º Contacto con grupos de interés especial

8º Revisión independiente de la SI

ii. Dispositivos móviles y trabajo remoto
   a) Objetivo: asegurar la SI cuando se usan medios de computación y teletrabajo móviles
   b) Controles
      1º Dispositivos móviles
      2º Trabajo remoto

7. Cláusula: recursos humanos
   - Objetivo
      i. Reducir riesgos de error humano, ilícitos, uso inadecuado de instalaciones y manejo no autorizado de información
      ii. Incluir responsabilidades sobre SI en el reclutamiento y en acuerdos de confidencialidad, y verificar su cumplimiento
      iii. Garantizar que los usuarios estén al corriente de las materias de SI y puedan respaldar la política
      iv. Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información
      v. Promover la comunicación de debilidades e incidentes con las herramientas y mecanismos necesarios
   - Categorías
      i. Antes del empleo
         a) Objetivo: asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y sean idóneos para sus roles
         b) Controles
            1º Funciones y responsabilidades
            2º Investigación de antecedentes
            3º Términos y condiciones de contratación
      ii. Durante el empleo
         a) Objetivo: asegurar que los empleados, contratistas y terceros sepan de las amenazas, sus responsabilidades y obligaciones, y puedan apoyar la política de SI
         b) Controles
            1º Responsabilidad de la dirección
            2º Concientización, formación y capacitación en SI
            3º Proceso disciplinario
      iii. Cese del empleo o cambio de puesto de trabajo
            1º Objetivo: asegurar que los empleados, contratistas y terceros salgan del organismo o cambien de empleo de manera ordenada
         b) Controles
            1º Responsabilidad del cese o cambio
            2º Devolución de activos

3º Retiro de los derechos de acceso

8. Cláusula: gestión de activos
    - Objetivo
        i. Garantizar que los activos de información tengan un apropiado nivel de protección
        ii. Clasificar la información según su sensibilidad y criticidad
        iii. Definir niveles de protección y medidas de tratamiento especial acorde a la clasificación
    - Categorías
        i. Responsabilidad sobre los activos
            a) Objetivo: activos inventariados y con propietario nombrado
            b) Controles
                1º Inventario de activos
                2º Propietario de activos
                3º Uso aceptable de activos
        ii. Clasificación de la información
            a) Objetivo: asegurar que la información reciba un nivel de protección apropiado
            b) Controles
                1º Directrices de clasificación
                2º Etiquetado y manipulado de la información
        iii. Gestión de medios
            a) Objetivo: evitar divulgación no autorizada, modificación, eliminación o destrucción de activos, e interrupción de actividades
            b) Controles
                1º Administración de medios informáticos removibles
                2º Eliminación de medios de información
                3º Seguridad de los medios de tránsito
9. Cláusula: gestión de accesos
    - Objetivo
        i. Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información
        ii. Controlar la seguridad en la conexión entre la red del organismo y otras redes
        iii. Concientizar a los usuarios de su responsabilidad con la utilización de contraseñas y equipos
        iv. Garantizar la SI cuando se utiliza computación móvil o instalaciones de trabajo remoto
    - Categorías
        i. Requerimientos para la gestión de acceso
            a) Objetivo: controlar el acceso a la información
            b) Controles

1º Política de gestión de accesos
2º Reglas de gestión de accesos

ii. Administración de gestión de usuarios
   a) Objetivo: controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información
   b) Controles
      1º Registración de usuarios
      2º Gestión de privilegios
      3º Gestión de contraseñas de usuario
      4º Administración de contraseñas críticas
      5º Revisión de derechos de acceso a usuarios

iii. Responsabilidades del usuario
   a) Objetivo: evitar el acceso no autorizado de usuarios, poner en peligro la información y el robo de información y los medios de procesamiento de información
   b) Controles
      1º Uso de contraseñas

iv. Control de acceso a sistemas y aplicaciones
   a) Objetivo: evitar el acceso no autorizado a los servicios de la red
   b) Controles
      1º Política de utilización de los servicios de red
      2º Camino forzado
      3º Autenticación de usuarios para conexiones externas
      4º Autenticación de nodos
      5º Protección de los puertos de diagnóstico remoto
      6º Subdivisión de redes
      7º Acceso a internet
      8º Conexión a la red
      9º Ruteo de red
      10º Seguridad de los servicios de red

v. Control de acceso al sistema operativo
   a) Objetivo: evitar el acceso no autorizado a los sistemas operativos
   b) Controles
      1º Identificación automática de terminales
      2º Procedimientos de conexión a terminales
      3º Identificación y autenticación de los usuarios
      4º Sistema de administración de contraseñas

10. Cláusula: criptografía
- Objetivo
   i. Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, no repudio, autenticidad y/o integridad
- Categorías

i. Cumplimiento de requisitos legales
    a) Objetivo: uso en base a un análisis de riesgo, desarrollando una política sobre el uso de controles criptográficos
    b) Controles
        1º Política de utilización de controles criptográficos
        2º Cifrado
        3º Firma digital
        4º Servicios de no repudio
        5º Protección de claves criptográficas
        6º Protección de claves criptográficas: normas y procedimientos

11. Cláusula: física y ambiental
- Objetivo
    i. Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del organismo
    ii. Proteger el equipamiento de procesamiento de información crítica ubicándolo en área protegidas, y también cuando esté fuera de las mismas
    iii. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático
    iv. Implementar medidas para proteger la información manejada por el personal en sus labores habituales
    v. Proporcional protección proporcional a los riesgos identificados
- Categorías
    i. Áreas seguras
        a) Objetivo: evitar el acceso físico no autorizado, daño e interferencia con la información y los locales del organismo
        b) Controles
            1º Perímetro de seguridad física
            2º Controles físicos de entrada
            3º Seguridad en las oficinas, despachos, instalaciones
            4º Protección contra amenazas externas y de origen ambiental
            5º Trabajo en áreas seguras
            6º Áreas de acceso público, de carga y descarga
    ii. Seguridad de los equipos
        a) Objetivo
            1º Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades
            2º Proteger el equipo de amenazas físicas y ambientales
        b) Controles
            1º Emplazamiento y protección de equipos
            2º Instalaciones de suministro
            3º Seguridad del cableado
            4º Mantenimiento de los equipos

5º Seguridad de los equipos fuera de las instalaciones
6º Reutilización o retiro seguro de los equipos
7º Retirada de materiales propiedad del organismo
8º Política de pantallas limpias
9º Política de escritorios limpios

12. Cláusula: seguridad en las operaciones
- Objetivo
    i. Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información
    ii. Establecer responsabilidades y procedimientos para su gestión y operación
- Categorías
    i. Procedimientos y responsabilidades operativas
        a) Objetivo
            1º Asegurar la operación correcta y segura de los medios de procesamiento de información
            2º Establecer las responsabilidades y procedimientos para la gestión de todos los medios
        b) Controles
            1º Documentación de los procedimientos
            2º Cambios en las operaciones
            3º Planificación de la capacidad
            4º Separación de entornos de desarrollo, pruebas y operacionales
    ii. Protección contra el malware (código malicioso)
        a) Objetivo: proteger la integridad del software. Evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados
        b) Controles
            1º Control contra el malware
            2º Código móvil
    iii. Resguardo (backup)
        a) Objetivo
            1º Mantener la integridad y disponibilidad de la información y los medios de procesamiento
            2º Establecer los procedimientos de rutina para implementar la política de respaldo y la estrategia para realizar copias de respaldo y practicar su restauración
        b) Controles
            1º Resguardo de la información
    iv. Registro y monitoreo
        a) Objetivo
            1º Detectar actividades de procesamiento no autorizadas

2º Monitorear los sistemas y reportar los eventos de seguridad de la información

b) Controles

1º Registro de eventos
2º Protección del registro de información
3º Registro del administrador y del operador
4º Sincronización de relojes

v. Control de software operacional

a) Objetivo

1º Garantizar la seguridad de los archivos del sistema
2º Controlar el acceso a los archivos del sistema y código fuente del programa, y los proyectos TI

b) Controles

1º Instalación de software en sistemas operacionales

vi. Administración de vulnerabilidades técnicas

a) Objetivo: implementar la gestión de vulnerabilidades técnicas de forma efectiva, sistemática y repetible, que incluyan los sistemas operativos y cualquier otra aplicación en uso

b) Controles

1º Administración de vulnerabilidades técnicas
2º Restricciones en la instalación de software

vii. Consideraciones sobre la auditoría de los sistemas de información

a) Objetivo: asegurar el cumplimiento de minimizar el impacto de las actividades de auditoría en los sistemas operacionales

b) Controles

1º Controles de auditoría en los sistemas de información

13. Cláusula: gestión de comunicaciones

- Objetivo
  i. Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones
- Categorías
  i. Gestión de la red
    a) Objetivo: asegurar la protección de la información en redes y la protección de la infraestructura de soporte
    b) Controles
      1º Redes
      2º Seguridad de servicio de red
  ii. Transferencia de información
    a) Objetivo: mantener la seguridad en el intercambio de información dentro del organismo y con cualquier entidad externa
    b) Controles
      1º Procedimientos y controles de intercambio de la información

2º Acuerdos de intercambio de información
3º Seguridad de la mensajería
4º Acuerdos de confidencialidad

14. Cláusula: adquisición, desarrollo y mantenimiento de sistemas
    - Objetivo
        i. Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de sistemas de información
        ii. Definir y documentar las normas y procedimientos a aplicar en el ciclo de vida de los aplicativos y la infraestructura en la que se apoyan
        iii. Definir los medios de protección de la información crítica o sensible
    - Categorías
        i. Requerimientos de seguridad de los sistemas
            a) Objetivo: garantizar que la seguridad sea una parte integral de los sistemas de información
            b) Controles
                1º Análisis y especificaciones de los requerimientos de seguridad
                2º Seguridad de servicios aplicativos en redes públicas
                3º Protección de servicios no aplicativos
        ii. Seguridad en los sistemas de información
            a) Objetivo: establecer controles y registros de auditoría, verificando la validación efectiva de los datos de entrada, el procesamiento interno, la autenticación de mensajes (interfaces entre sistemas) y la validación de datos de salida
            b) Controles
                1º Validación de datos de entrada
                2º Controles de procesamiento interno
                3º Autenticación de mensajes
                4º Validación de datos de salida
        iii. Seguridad en los archivos del sistema
            a) Objetivo: garantizar que los desarrollos y las actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo
            b) Controles
                1º Software operativo
                2º Protección de los datos de prueba del sistema
                3º Cambios a datos operativos
                4º Acceso a las bibliotecas de programas fuentes
        iv. Seguridad en los procesos de desarrollo y soporte
            a) Objetivo: controlar los entornos y el soporte dado a los mismos
            b) Controles
                1º Procedimiento de control de cambios

2º Revisión técnica de los cambios en el sistema operativo
3º Restricción del cambio de paquetes de software
4º Canales ocultos y código malicioso
5º Desarrollo externo de software

v. Gestión de vulnerabilidades técnicas
a) Objetivo: implementarla de forma efectiva, sistemática y repetible, incluyendo sistemas operativos y cualquier otra aplicación en uso
b) Controles
1º Vulnerabilidades técnicas

15. Cláusula: relaciones con proveedores
- Objetivo
i. Establecer y mantener el nivel acordado de SI y prestación de servicios conforme a los acuerdos del proveedor
- Categorías
i. Seguridad de la información en las relaciones con el proveedor
a) Objetivo: garantizar y asegurar la protección de la información del organismo que es accedida por los proveedores
b) Controles
1º Política de SI para las relaciones con el proveedor
2º Abordar la seguridad dentro de los acuerdos del proveedor
3º Cadena de suministro de tecnologías de la información y comunicaciones
ii. Administración de prestación de servicios de proveedores
a) Objetivo: garantizar el mantenimiento del nivel acordado de SI y prestación de servicios conforme a los acuerdos del proveedor
b) Controles
1º Supervisión y revisión de los servicios del proveedor
2º Gestión de cambios a los servicios del proveedor

16. Cláusula: gestión de incidentes de seguridad
- Objetivo
i. Garantizar que se comuniquen los incidentes y debilidades para que se apliquen las acciones correctivas oportunamente
- Categorías
i. Informe de los eventos y debilidades de la seguridad de la información
a) Objetivo: asegurar que se comuniquen los incidentes y debilidades para que se apliquen las acciones correctivas oportunamente
b) Controles
1º Reporte de los eventos de la SI
2º Reporte de las debilidades de la seguridad
3º Comunicación de anomalías del software
ii. Gestión de los incidentes y mejoras de la seguridad de la información

a) Objetivo: asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes
b) Controles
    1º Responsabilidades y procedimientos
    2º Aprendiendo a partir de los incidentes
    3º Procesos disciplinarios

17. Cláusula: gestión de la continuidad

- Objetivo
    i. Minimizar los efectos de las posibles interrupciones de las actividades del organismo y proteger los procesos críticos mediante controles preventivos y acciones de recuperación
    ii. Analizar las consecuencias de la interrupción del servicio y tomar medidas para prevenir hechos similares en el futuro
    iii. Asegurar la coordinación con el personal del organismo y contactos externos que participarán en la planificación de contingencias
    iv. Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes
- Categorías
    i. Gestión de continuidad del organismo
        a) Objetivo: contraatacar las interrupciones a las actividades del organismo y proteger los procesos críticos, y asegurar su reanudación oportuna
        b) Controles
            1º Proceso de administración de continuidad del organismo
            2º Continuidad de las actividades y análisis de los impactos
            3º Elaboración e implementación de los planes de continuidad de las actividades
            4º Marco para la planificación de la continuidad de las actividades del organismo
            5º Ensayo, mantenimiento y reevaluación de los planes de continuidad del organismo
    ii. Redundancias
        a) Objetivo: asegurar la continuidad de la información y que esté integrada a los sistemas de gestión
        b) Controles
            1º Disponibilidad de las instalaciones de procesamiento de la información

18. Cláusula: cumplimiento

- Objetivo
    i. Cumplir con las disposiciones normativas y contractuales para evitar sanciones al organismo y/o al empleado

ii. Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad
iii. Revisar la seguridad de los sistemas de información periódicamente
iv. Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo
v. Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas
vi. Determinar los plazos para el mantenimiento de información y la recolección de evidencia del organismo

- Categorías
    i. Cumplimiento de requisitos legales
        a) Objetivo: evitar las violaciones a cualquier ley, regulación y cualquier requerimiento de seguridad
        b) Controles
            1º Identificación de la legislación aplicable
            2º Derechos de propiedad intelectual
            3º Protección de los registros del organismo
            4º Protección de datos y privacidad de la información personal
            5º Prevención del uso inadecuado de los recursos de procesamiento de información
            6º Regulación de controles para el uso de criptografía
            7º Recolección de evidencia
            8º Delitos informáticos
    ii. Revisiones de política de seguridad y la compatibilidad técnica
        a) Objetivo: asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional
        b) Controles
            1º Cumplimiento de la política de seguridad
            2º Verificación de la compatibilidad técnica
    iii. Consideraciones de auditoría de sistemas
        a) Objetivo
            1º Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información
            2º Durante las auditorías de los sistemas de información deberían existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría
        b) Controles
            1º Controles de auditoría de sistemas
            2º Protección de los elementos utilizados por la auditoría de sistemas
            3º Sanciones previstas por incumplimiento