Procedimientos De Seguridad De La Información

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 3

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	25/04/2016	Versión inicial del documento

TABLA DE CONTENIDO

PÁG.

1. DERECHOS DE AUTOR

2. AUDIENCIA

Entidades públicas de orden nacional y territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

Esta estrategia se fundamenta en cuatro componentes, TIC para servicios, TIC para gobierno abierto, TIC para la gestión y seguridad y privacidad de la información, a través de los cuales se busca facilitar la masificación de la oferta y demanda del Gobierno en Línea.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha diseñado un documentos de lineamientos “Modelo de Seguridad y Privacidad de la Información” el cual lo largo de los últimos años se ha ido actualizando en función de las modificaciones de la norma técnica que le sirve de sustento: ISO 27001, las mejores prácticas y los cambios normativos que tengan impacto sobre el mismo.

A su turno el Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

4. OBJETIVOS

La presente guía tiene como objetivo principal, indicar los procedimientos de seguridad que pueden generarse durante el diseño y la implementación del modelo de seguridad y privacidad de la información para las entidades del estado.

Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente.

5. GLOSARIO

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustaran a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Instructivo: Documento que describe de una manera detallada cómo debe ejecutarse una actividad o tarea determinada para garantizar su realización, hablan sobre métodos específicos sobre plataformas, sistemas de información o algún proceso definido.

6. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En este documento presenta algunas recomendaciones de procedimientos de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para las Entidades del Estado.

El conjunto de procedimientos que se presentará a continuación, constituye una base sólida para que cada entidad genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar.

Con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad, se tomaron en cuenta los 14 numerales de control de seguridad de la información definidas en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios.

Es importante aclarar que en los procedimientos, se pueden citar instructivos o documentos informativos adicionales como complemento.
Así mismo, la complejidad o extensión de cada procedimiento dependerá del tipo de entidad y los recursos de los cuales disponga.

6.1 SEGURIDAD DEL RECURSO HUMANO:

En este dominio relacionado con el personal que labora dentro de la entidad, se pueden definir los siguientes procedimientos:

- **PROCEDIMIENTO DE CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL:** Indica la metodología empleada por la entidad para realizar la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades, la periodicidad de dichas capacitaciones y sensibilizaciones etc…
- **PROCEDIMIENTO DE INGRESO Y DESVINCULACIÓN DEL PERSONAL:** Este procedimiento indica la manera como la entidad gestiona de manera segura el ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad, recepción de entregables requeridos para generar paz y salvos entre otras características. **Este procedimiento va de la mano con el área de gestión de recursos humanos o contratación puede generarse con su colaboración.**

6.2 GESTION DE ACTIVOS:

En este dominio relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad se pueden definir los siguientes procedimientos:

- **PROCEDIMIENTO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS:** En este procedimiento se debe indicar la manera en que los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son clasificados de acuerdo a su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad.

  Adicionalmente se debe explicar cómo se hace una correcta disposición de los activos cuando ya no se requieran y su transferencia hacia otros lugares de manera segura.

6.3 CONTROL DE ACCESO:

En este dominio relacionado con el acceso a la información y a las instalaciones de procesamiento de la información, se pueden generar los siguientes procedimientos:

- **PROCEDIMIENTO PARA INGRESO SEGURO A LOS SISTEMAS DE INFORMACIÓN:** En este procedimiento la entidad debe indicar como gestiona el acceso a sus sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza bruta, validando los datos completos para ingreso a los sistemas, empleando métodos para cifrar la información de acceso a través de la red entre otros.
- **PROCEDIMIENTO DE GESTIÓN DE USUARIOS Y CONTRASEÑAS:** En este procedimiento, la entidad deberá indicar como realiza la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de las mismas. Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.

6.4 CRIPTOGRAFÍA:

En este dominio está relacionado con el buen uso de la criptografía para garantizar la disponibilidad, integridad y confidencialidad de la información, así como también el correcto uso de las llaves criptográficas durante todo su ciclo de vida (creación, uso, recuperación, distribución, retiro y destrucción. Se pueden generar los siguientes procedimientos:

- **PROCEDIMIENTO DE CONTROLES CRIPTOGRÁFICOS:** En este procedimiento deberá especificarse como se utilizará la criptografía dentro de los sistemas de información de la organización para garantizar su integridad, disponibilidad y confidencialidad.
  Debe especificarse la complejidad de los controles criptográficos a emplear, dependiendo de la criticidad de la información que circulará a través de la red o se encontrará alojada en un sistema determinado.
- **PROCEDIMIENTO DE GESTIÓN DE LLAVES CRIPTOGRÁFICAS:** Este procedimiento deberá describir el ciclo de vida de las llaves criptográficas dentro de la entidad (si aplica), desde que se crean hasta que se distribuyen a cada usuario o aplicación de manera segura. Deben mencionarse aspectos como la creación de las llaves, obtención de certificados, almacenamiento seguro de las llaves, actualización o cambio, revocación y recuperación de llaves.

6.5 SEGURIDAD FÍSICA Y DEL ENTORNO:

Este dominio está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información. Se pueden generar los siguientes procedimientos (**estos procedimientos pueden tener la participación del área de seguridad y vigilancia de la entidad**):

- **PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO:** En este procedimiento se debe describir como se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permiso a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a las áreas etc…
- **PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS:** Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la

entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas etc…

- **PROCEDIMIENTO DE RETIRO DE ACTIVOS:** En este procedimiento debe especificarse como los activos son retirados de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos etc.…)
- **PROCEDIMIENTO DE MANTENIMIENTO DE EQUIPOS:** Este procedimiento debe especificar como se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, indicando los intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores o si existen seguros atados a los equipos y los mantenimientos sean requisitos. Se debe especificar el modo en que los mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.

6.6 SEGURIDAD DE LAS OPERACIONES:

Este dominio busca asegurar las operaciones correctas dentro de las instalaciones de procesamiento de información:

- **PROCEDIMIENTO DE GESTIÓN DE CAMBIOS:** En este procedimiento la entidad deberá como realiza el control de cambios en la organización, los procesos de negocio y los sistemas de información de manera segura. Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa) entre otros.

- **PROCEDIMIENTO DE GESTION DE CAPACIDAD:** Se debe especificar como la organización realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son excasos, demorados en su arribo o costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc…

- **PROCEDIMIENTO DE SEPARACIÓN DE AMBIENTES:** Con el fin de evitar problemas operacionales que pueden desencadenar en incidentes críticos, es necesario desarrollar un procedimiento de separación de ambientes que permita realizar una transición de los diferentes sistemas desde el ambiente de desarrollo hacia el de producción. Dentro de los aspectos más importantes a considerar se encuentran la implementación de un ambiente de pruebas para las aplicaciones, definición de los requerimientos para la transición entre ambientes, la compatibilidad de los desarrollos con diferentes sistemas entre otros.
- **PROCEDIMIENTO DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS:** La entidad debe indicar por medio de este procedimiento como realiza la protección contra códigos maliciosos teniendo en cuenta, que controles utiliza (hardware o software), como se instalan y se actualizan las plataformas de detección, definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso, implementación de procedimientos para recolectar información de manera regular como suscripción a listas de correo

6.7 SEGURIDAD DE LAS COMUNICACIONES:

Este dominio busca el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización.

- **PROCEDIMIENTO DE ASEGURAMIENTO DE SERVICIOS EN LA RED:** Este procedimiento explica la manera en que la entidad protege la información en las redes, indicando los controles de seguridad (como se cifran los datos a través de la red por ejemplo) que se aplican para acceder a la red cableada e inalámbrica, satelital etc… con miras a proteger la privacidad de la información que circula a través de estos medios, también se debe incluir el uso de registros (logs) que permitan realizar seguimiento a acciones sospechosas.

- **PROCEDIMIENTO DE TRANSFERENCIA DE INFORMACIÓN:** En este procedimiento la entidad deberá indicar como realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.
  Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan

condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

6.8 RELACIONES CON LOS PROVEEDORES:

Este dominio está relacionado con la protección de los activos de la organización a los cuales los proveedores o terceros tienen acceso.

- **PROCEDIMIENTO PARA EL TRATAMIENTO DE LA SEGURIDAD EN LOS ACUERDOS CON LOS PROVEEDORES:** Este procedimiento debe indicar como la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos tengan (es decir algún intermediario). Dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.

6.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN:

- **PROCEDIMIENTO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE:** Este procedimiento deberá describir como se realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (inhouse) o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad.

  Se deben tener en cuenta el uso de ambientes de desarrollo, pruebas y producción para los sistemas de información.

- **PROCEDIMIENTO DE CONTROL SOFTWARE:** En este procedimiento la entidad deberá indicar como realiza el control de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad,

quienes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

6.10 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

- **PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:** Este procedimiento debe indicar como responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad. Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes De Continuidad) dependiendo de la criticidad de la información.

6.11 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO:

- **PROCEDIMIENTO DE GESTIÓN DE LA CONTINUIDAD DE NEGOCIO:** En este procedimiento la entidad debe indicar la manera en que la entidad garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico.

  El procedimiento debe indicar los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal.

7. FORMATO EJEMPLO PARA ELABORACIÓN DE PROCEDIMIENTOS

A continuación se muestra un formato ejemplo para realizar procedimientos, está basado en un modelo del ***Ministerio Del Interior.***

Es importante agregar que los procedimientos pueden a su vez citar otros documentos adicionales que complementen mejor la descripción del mismo, como por ejemplo:

- Instructivos
- Reglas
- Políticas
- Informativos

LOGO	PROCEDIMIENTO _____	**Código:** Código Del Procedimiento/Nemónico
		Versión: Versión Del Procedimiento
		Fecha Creación:
		Fecha De Aprobación:

1. OBJETIVO

2. ALCANCE

3. DEFINICIONES

4. SIGLAS

5. NORMATIVIDAD
***5*.1. CONSTITUCIÓN.**
5.2. LEYES.
5.3. DECRETOS.
5.4. RESOLUCIONES.

5.5. OTRAS
Por ejemplo normas o estándares.

6. DESARROLLO

No.	Actividad	Tarea	Punto De Control	Responsable
1				
2				
3				
4				
5				

Actividad: Paso a ejecutarse.
Tarea: Descripción detallada de la actividad incluyendo labores adicionales para explicar detalladamente el proceso.

Punto De Control: Requerimiento mínimo para que la actividad pueda ejecutarse, por ejemplo un control de cambios, un formato o una aprobación.
Responsable: Responsable de la actividad

7. REGISTROS

Posibles documentos de salida.

8. INFORMACIÓN

INFORMACIÓN GENERADA	RESPONSABLE	FRECUENCIA	UBICACIÓN

9. SISTEMAS DE INFORMACIÓN

SISTEMA DE INFORMACIÓN	DESCRIPCIÓN	RESPONSABLE	UBICACIÓN

10. ANEXOS

Pueden referenciarse formatos, instructivos, informativos, reglas etc…

11. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN

Elaboró **Revisó y Aprobó**

_____ _____

8. BIBLIOGRAFÍA

- ISO/IEC 27002, Information Technology. Security Techniques. *Code of practice for information security controls.*