Objetivo General: Revisar la normatividad administrativa propuesta por las Unidades Administrativas emisoras, mediante la revisión del marco normativo y la calidad regulatoria.

Generalidades

Nombre de las disposiciones:

1. Directrices de seguridad de la información.
2. Directrices de seguridad de la información de TIC.
3. Directrices de uso y operación del correo electrónico institucional.

Periodo de revisión: Del 4 al 17 de febrero de 2016.

Desarrollo

Derivado del análisis al documento, se presentan de manera general los comentarios y/o sugerencias siguientes:

Directrices de uso y operación del correo electrónico institucional.

General

De la misma manera que los documentos anteriores, se considera conveniente definir el instrumento normativo a aplicar, por lo que se sugiere valorar que su contenido forme parte de un sólo documento que reúna las directrices de seguridad establecidas en el MAAGTICSI.

*Introducción. S*e menciona a la población objetivo responsable de la aplicación; sin embargo, se sugiere reubicar al apartado denominado Responsables de la aplicación.

Por otra parte se indica que el documento que nos ocupa forma parte del documento maestro de Directrices de Seguridad de la Información de las Directrices de TIC, lo cual confirma la sugerencia de este OIC para unificar un solo documento.

Responsables de aplicación

Se limita la aplicación del documento a una unidad administrativa, cuando el uso del correo electrónico se presenta prácticamente en todos los niveles de la SCT.

Actualización del documento

Para la actualización del documento, se menciona la figura de Grupo Estratégico de Seguridad de la Información (GESI), la cual difiere a la señalada en las Directrices de seguridad de la información de TIC y Directrices de seguridad de la información, se sugiere revisar y definir la correcta, tomando como referencia la acreditación de su creación y operación en la SCT.

Por otra parte, se hace mención que la disposición podrá actualizarse sin previo aviso, lo cual es improcedente toda vez que la disposición normativa debe ser sujeta a un proceso de calidad regulatoria. Asimismo, existe incertidumbre de la responsabilidad del diseño de la disposición, debido a que se hace mención al GESI y a la UTIC.

Se hace mención a la integración del GESI; sin embargo, se sugiere no mencionarlo debido que se duplicaría con el documento de integración y operación del GESI que establece el responsable de la seguridad de la información en la institución (RESII).

Definiciones. Fortalecer el apartado, considerando que se indican definiciones en otros apartados de la disposición.

Descripción Técnica del Servicio de Correo Electrónico. Se debe limitar el contenido a aspectos que agreguen valor a dicho apartado y no así a definiciones.

Responsabilidad de los servicios. Se señalan responsabilidades de diversas figuras jurídicas, las cuales pueden formar parte del manual de organización de la unidad administrativa o en su defecto de los lineamientos de operación del Grupo Estratégico de Seguridad de la Información (GESI).

Directrices.- Se sugiere revisar de manera general, toda vez que algunos puntos que no son claros y crean confusión al usuario a quien va dirigido.

Firmas del documento. Al estar firmado el documento por diferentes servidores públicos se presume que ya está autorizado, hecho contrario a la realidad, debido a apenas se está revisando.

Considerando que el establecimiento de directrices de seguridad de la información pueden ser complementadas con base en mejores prácticas y estándares internacionales en la materia; sin embargo, no se aprecia alguna disposición en el marco jurídico que se haya considerado para su diseño o que se transite a la certificación por la Norma ISO/IEC/27001.

¿Qué es la norma ISO 27001?

La norma adopta una aproximación de proceso al establecimiento, a la implementación, a la operación, el monitoreo, a la revisión, al mantenimiento y a la mejora del sistema de gestión de seguridad de la información de una organización.

La Organización Internacional de Estandarización (ISO) estableció la norma ISO 27001, la cual se emplea para la certificación. Ha reemplazado el estándar BS 7799 y brinda una norma internacional para sistemas de gestión de seguridad de la información. Con base en el estándar BS 7799, se la ha reorganizado para alinearse con otras normas internacionales. Se han incluido algunos nuevos controles, es decir, el énfasis en las métricas para la seguridad de la información y la gestión de incidentes.

La norma también se fundamenta en otras como ISO/IEC 17799:2005, la serie ISO 13335, ISO/IEC TR 18044:2004 y las "Directrices de la OCDE para Sistemas y Redes de Seguridad de la Información – Hacia una cultura de seguridad" que proporcionan orientación para la implementación de la seguridad de la información.

En conformidad con otras normas de sistemas de

La norma ISO 27001 está alineada con otros sistemas de gestión y soporta la implementación y la operación coherente e integrada con normas de gestión relacionadas. El resultado es:

- Armonización con normas de sistemas de gestión como ISO 9001 e ISO 14001.
- Énfasis en la mejora continua de procesos de su sistema de gestión de seguridad de la información.
- Clarificación de requisitos de documentación y registros.
- Procesos de evaluación y gestión de los riesgos involucrados mediante la utilización de un modelo del proceso PDCA - Planificar, Hacer, Verificar, Actuar (PDCA, por sus siglas en inglés).

Comentarios generales para la emisión de los documentos.

La implementación de Políticas de Seguridad de la Información es un proceso técnico y administrativo que debe abarcar a toda la Institución, por ende, debe estar avalado y contar con un fuerte apoyo de la alta dirección, ya que sin este apoyo, su implementación será más compleja e incluso puede no tener el éxito esperado.

Es importante que al momento de formular dichas políticas, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los recursos existentes, así como adecuar las políticas a la realidad de la Dependencia.

- Reunirse con las unidades administrativas, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir los riesgos en su incumplimiento.

- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas establecidas.