LINEAMIENTOS EN MATERIA DE SEGURIDAD INFORMATICA

I.- INTRODUCCIÓN.

Con el propósito de mejorar los niveles de seguridad tanto del personal de la DGTII y de los recursos informáticos de la Secretaría de Relaciones Exteriores, se establecen los presentes Lineamientos en Materia de Seguridad Informática, que se detallan en el presente documento.

II.- MARCO JURÍDICO.

1.- Ley Orgánica de la Administración Pública Federal.
2.- Ley General de Bienes Nacionales
3.- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
4.- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
5.- Reglamento Interior de la Secretaría de Relaciones Exteriores.
6.- Condiciones Generales de Trabajo de la Secretaría de Relaciones Exteriores.

III.- SUJETOS DE LINEAMIENTO.

Los presentes lineamientos son de observancia general y obligatoria para todas las áreas de la Dirección General de Tecnologías de Información e Innovación (DGTII) y el personal adscrito a las mismas. La inobservancia, en lo conducente, de los presentes lineamientos será causal de las responsabilidades administrativas, civiles o penales que correspondan.

IV.- LINEAMIENTOS

A. ACCESO FISICO

1. El centro de Datos de la SRE es considerada un área de acceso restringido exclusivo a personal que por sus funciones requiera acceso al mismo. Será responsabilidad de la Dirección Adjunta de Operación de Tecnologías de la Información (DGAOTI), a través de la Dirección de Infraestructura y Telecomunicaciones (DIT) establecer un control de acceso físico al interior del centro de Datos de la SRE, así como llevar el registro de visitas como evidencia del cumplimiento del lineamiento.

2. Las área donde se localizan las plantas eléctricas, equipamiento de telecomunicaciones, UPS's y tableros eléctricos son también consideradas áreas de

acceso restringido. Será responsabilidad de la Dirección Adjunta de Operación de Tecnologías de la Información (DGAOTI), a través de la Dirección de Infraestructura y Telecomunicaciones (DIT) establecer un control de acceso físico al interior de las mismas.

3. El centro de datos deberá contar con un sistema de alarma ante caso de incendio o sismo que permita la coordinada evacuación del personal que labora al interior de manera eficiente.

4. El personal que labore al interior de las áreas restringidas deberá conocer el plan de evacuación que la Secretaría tenga vigente.

B. ACCESO LOGICO

1. Para hacer uso de los recursos informáticos disponibles en la SRE, un sujeto deberá realizar el acceso a los sistemas a través de una cuenta única de usuario, existiendo una relación única entre el sujeto y su cuenta, esto a fin de autenticar al sujeto, la DGAOTI será la responsable de administrar el sistema de control de accesos lógico.

2. Se debe establecer los mecanismos para la protección y los derechos de acceso a los recursos (sistemas informáticos y Datos) con el fin de controlar el acceso de sujetos (Programas, procesos o usuarios), así como la utilización de los mismos, garantizando la confidencialidad e integridad de dichos recursos.

3. No deberán existir cuentas de usuarios genéricas (usuarios agrupados bajo una sola contraseña compartida) para el uso de recursos.

4. Para los recursos informáticos como servicio de internet, su uso es exclusivo para temas laborales o de índole diplomático quedando prohibido por seguridad su uso para accesos de temas que fomenten la discriminación, pornografía y sitios catalogados con contenido de tipo malicioso (malware).

5. El resguardo de la contraseña ligada a una cuenta de usuario, es responsabilidad de la persona asignada a la misma, por lo cual, no se podrá revelar ni compartir la contraseña a un tercero.

6. Las contraseñas no podrán exhibirse en forma alguna, ni resguardarles en archivos sin encriptar, a fin de evitar que un sujeto externo o ajeno pueda acceder a ella.

7. La contraseña ligada a una cuenta de usuario deberá modificarse de manera frecuente dentro de un periodo establecido.

8. La cuenta de usuario deberá inhabilitarse de manera temporal después de un número de intentos consecutivos fallidos predeterminado por parte del sujeto, el cual intenta autenticarse a los recursos.

9. El resguardo de contraseñas vinculadas a cuentas especiales será responsabilidad de la Dirección General Adjunta de Seguridad Tecnológica (DGAST) y proporcionará dicha contraseña en función a criterios establecidos a los usuarios de la misma (sujetos).

10. Los accesos lógicos serán realizados a través de los equipos que la Dirección de Servicios Informáticos (DSI) asigne para este fin, así mismo, la DSI establecerá los lineamientos necesarios para regular el uso de los equipos, el soporte que se preste a todos los recursos informáticos y que garantice la integridad de la información contenida en los mismos.

a. Acceso Remoto

- Todo acceso de un sujeto a los recursos de manera remota desde cualquier lugar deberá ser a través de una conexión segura por Internet (VPN).

- Se deberá controlar el acceso de sujetos a los recursos a través de un túnel creado en Internet con el uso de una aplicación (Virtual Private Network), así como de la cuenta de usuario asignada al sujeto. Sera la DGAST la responsable del control y administración de usuario de acceso remoto.

- Se deberá considerar los siguientes lineamientos para dicho proceso:

    - Solo existirá una conexión por personal.
    - La sesión una vez alcanzando un periodo de inactividad establecida será desconectada del recurso.
    - Los equipos utilizados por los sujetos para un acceso remoto, utilizarán software antivirus.
    - Mediante el uso de la tecnología de acceso remoto, las computadoras utilizadas para dicho fin (institucionales o personales) estarán sujetas a las mismas normas y reglamentos dentro de la DGTII.
    - La persona a la que sea asignada una VPN deberá de firmar una carta responsiva donde asume los deberes y obligaciones de uso de la información accesada por la VPN en cuestión.

b. Puesto de trabajo

- Cuando se abandone el puesto de trabajo, la terminal asignada para realizar las funciones se deberá bloquear de modo obligatorio antes de abandonar la misma.

- Los equipos o terminales que no registre actividad por un periodo máximo de 10 minutos, éstas deberán desactivarse a través de un “protector de pantalla”.

- La activación de los equipos o terminales deberá ser por medio de contraseña.

- La DSI deberá procurar que los equipos o terminales utilizadas para realizar las funciones de los usuarios tengan contraseña de arranque, configuradas en la BIOS.

c. AUTENTICACIÓN

1. Se deberá establecer la validación o autenticación como mecanismo para permitir o denegar el acceso a los sistemas, así como para negar una transacción proveniente de alguien no autorizado.

2. La Dirección General Adjunta de Arquitectura y Diseño de Tecnologías de Información (DGAADTI) a través de sus Direcciones de Arquitectura Aplicativa (DAA) y Arquitectura de Sistemas (DAS) garantizarán que todo el software desarrollado tenga control de acceso lógico a través de un método de autenticación

3. El proceso de validación deberá minimizar las falsas aceptaciones o entradas no autorizadas a los sistemas, así como los falsos rechazos, esto mediante la utilización de mecanismos autenticación (contraseña, credenciales, etc.) para lograr el acceso a los sistemas.

4. Para verificar la identidad del sujeto y por lo tanto ganar el acceso a los recursos como sujeto autorizada, deberá existir una cuenta única de usuario vinculada al sujeto, es decir, existirá una relación única entre la persona y su cuenta.

5. Para fortalecer el método de autenticación por contraseña deberá observarse lo siguiente:

    - La contraseña será construida con una longitud de al menos de ocho caracteres.
    - La construcción será una mezcla aleatoria de caracteres alfabéticos, especiales y numéricos.
    - Los caracteres alfabéticos utilizarán mayúsculas y minúsculas.
    - La construcción no partirá de lo siguiente: Una palabra común del lenguaje o de la jerga, el nombre del sujeto o usuario, pariente o de la información

personal del usuario (número telefónico, número de identificación, fecha de nacimiento, etc.)
- La contraseña construida será significativamente diferente respecto de otras contraseñas anteriormente creadas (relación de caracteres utilizados).

6. Se deberá establecer los métodos apropiados de autenticación remota (conexión) a través de del intercambio de credenciales para cada una de las partes en la conexión a fin de autenticar al sujeto y establecer la conexión segura.

d. AUTORIZACIÓN E INTEGRIDAD

1. Para la utilización de los recursos por parte de los usuarios, se debe establecer diferentes niveles de autorización (privilegio) con el objeto de poder realizar operaciones sobre los recursos con derecho de acceso.

2. Cada usuario deberá tener el mínimo de privilegios requeridos a fin de realizar sus funciones de acuerdo a su perfil establecido, bajo los siguientes lineamientos:

    - Para poder realizar las funciones asignadas se procurará satisfacer las propiedades del perfil de acuerdo a los derechos de acceso requeridas para la misma.

    - La opción por omisión o no expresar el acceso a algo, significa todo está restringido, a menos que este expresamente permitido el acceso al recurso.

    - Minimizar el uso de recursos compartidos.

3. Los privilegios asignados a un sujeto para ejecutar ciertas operaciones sobre los recursos deberá basarse en los derechos de acceso (protección) sobre cada recurso.

4. Se debe implantar los controles para prevenir el acceso no autorizado de terceros a los datos sensibles de la Organización con el fin de garantizar la confidencialidad, no repudio y la integridad de la misma, debido a las vulnerabilidades existentes en el uso de conexiones públicas o datos sin codificación.

C. CLASIFICACION DE INFORMACIÓN

1. Toda la información contenida en equipos a cargo de la DGTII deberá estar clasificada siguiendo los lineamientos que se han establecidos en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

2. La DGADTI será la responsable de solicitar a las áreas propietarias de la información la clasificación de la misma para que esta sea informada a la DGTII y se tomen las medidas de protección pertinentes.

D. CONFIDENCIALIDAD

1. Todos los funcionarios, personal de honorarios, becarios o proveedores adscritos a la DGTII deberán firmar una responsiva de confidencialidad donde se comprometan a mantener de manera confidencial la información que tienen a su cargo.

2. No está permitido hacer referencia a temas o información oficial y confidenciales de la SRE en público o la distribución de mismos por medio de cualquier dispositivo o canal de comunicación no controlados por la DGTII.

3. La información sensible transferida a cualquier dispositivo móvil (laptops y tablets) debe estar cifrada de acuerdo a los lineamientos establecidos, a las leyes y reglamentos correspondientes.

4. Los usuarios con capacidad de acceso remoto a través de VPN asumen la responsabilidad del buen uso de este recurso y deberán tomar las medidas de prevención adicionales para asegurar el adecuado manejo de los recursos sensibles.

5. La información sensible almacenada en equipos personales de la DGTII, deberá estar cifrada o cuando ésta sea copiada, asimismo la información sensible transmitida a través de redes públicas será enviada de manera cifrada.

6. Los equipos virtuales establecidos como estratégicos deberá sujetarse a la presente políticas de cifrado de la información.

7. Los mecanismos de la tecnología de cifrado deberán configurarse de acuerdo a las mejores prácticas de acuerdo a los marcos de referencia existentes, garantizando la efectividad contra posibles violaciones.

8. El Grupo Estratégico de Seguridad de la Información o GESI deberá determinar las siguientes condiciones en cuanto al cifrado de información:

    - Identificar la información o grupo de datos sensibles de la DGTII para su cifrado.

- Grupo de sujetos especiales con acceso o manejo de información sensible candidatos a cifrar la información de sus equipos personales.

- Las claves de cifrado estarán al resguardo de la DGTII y cualquier solicitud de cambio para dicha clave será bajo los criterio establecidos por la DGTII.

Transferencia de Información

1. Deberán existir mecanismos para evitar el envío de información sensible por parte de los sujetos a fin de identificar, supervisar y proteger los mismos, y de esta manera prevenir el uso no autorizado y la transmisión de información sensible.

2. Los medios de comunicación, es decir, los enlaces de datos de las redes privadas de la Secretaría deberán de establecer mecanismos entre locaciones con el fin de cifrar el medio.

3. Las aplicaciones y portales que la Secretaría ofrece a los usuarios internos y a la ciudadanía serán cifrados obligatoriamente a través de certificados SSL el cual será obtenido por medio de una entidad certificadora interna y/o externa.

E. INCIDENTES DE SEGURIDAD

1. Los eventos de seguridad deberán ser registrados y monitorizados, examinando los registros en bitácora de indicadores de actividades no autorizadas relacionadas con la seguridad, de esta manera, ayudando a proteger la información sensible y a través de un análisis cuidadoso de tendencias, identificar mejoras al programa de gestión de la seguridad.

2. La violación de los lineamientos de uso de los recursos informáticos de la SRE constituye un incidente de seguridad que deberá de ser tratado de acuerdo a los lineamientos del MAAGTICSI.

3. Se deberá contar con un procedimiento de eventos de seguridad el cual se sustente en los procesos ASI de MAAGTICSI para reunir los datos de los eventos, de las amenazas y de los riesgos, así como la revisión de dichos registros para proporcionar:

    - Información sobre la seguridad.
    - Lograr respuestas rápidas a los incidentes.
    - Gestionar los registros almacenados.
    - Generar reportes de cumplimiento.

4. El objeto del proceso de eventos de seguridad deberá ser el de encontrar eventos correlacionados, tales como:

- Acceso individual a la información sensible.
- Todas las acciones realizadas por cuentas privilegiadas.
- Acceso a los datos y funciones de la pista de auditoria.
- Intentos inválidos de accesos lógicos.
- Todas las acciones de identificación y autenticación.
- Creación y eliminación de objetos a nivel del sistema.

Asimismo, del aprendizaje obtenido, las posibles acciones incluyen:

- Aplicar los controles apropiados.

- Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos, como es indicado en el numeral 3.

- Evitar los riesgos.

- Transferir a otras partes los riesgos asociados con las actividades de la organización, por ejemplo: aseguradoras y proveedores.

Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.

- Se deben seleccionar e implantar los objetivos de control, así como los controles para cumplir con los requerimientos identificados en el proceso de valoración y tratamiento de riesgos.

F. PROVEEDORES EXTERNOS

1. Todas las áreas que contraten servicios administrados al interior de la DGTII deberán garantizar que los contratos correspondientes tiene definido de manera clara los niveles de servicio que serán otorgados, así como las penalizaciones en caso de incumplimiento de los mismos.

2. Todos los contratos con proveedores externos deberán contener cláusulas de confidencialidad que obliguen al personal en sitio el mantener la confidencialidad, integridad y disponibilidad de la información al interior de la SRE.

3. Todos los contratos con proveedores externos deberán contener una cláusula que garantice que el personal asignado a la Secretaría ha sido sometido a análisis de

confianza que indiquen que dicho personal no tiene antecedentes penales o que su perfil psicométrico lo vuelve apto para desempeñar las funciones conferidas.

4. Todos los contratos con proveedores externos deberán contener una cláusula que permita imponer penalizaciones hasta la recisión del contrato en caso de que el personal de dicho proveedor se vea involucrado en un incidente de seguridad que sea catalogado como de alto riesgo según lo establezca el ERISC.

G. MONITOREO DE ACTIVOS DE TIC (PISTAS DE AUDITORIA)

1. Todas las áreas de la DGTII serán responsables de implementar y activar sistemas de monitoreo que permitan al adecuada vigilancia de niveles de servicio y seguridad de las infraestructuras de Tecnologías de Información y Comunicaciones.

2. Cada área deberá almacenar las bitácoras o registros necesarios que permitan demostrar el buen desempeño de procesos y acceso a la infraestructura informática. Dichos registros deberán mantenerse por el periodo que cada área determine pertinente para una adecuada operación y deberán estar a disposición cuando sean requeridos debido a un proceso de auditoría o investigación de incidente de seguridad.

3. La DAST deberá establecer un monitoreo de Seguridad que detecte vulnerabilidades técnicas sobre la plataforma existente en la Secretaría de manera periódica. Las vulnerabilidades detectadas deberán ser comunicadas a las áreas responsables de dicha infraestructura y/o sistemas para que puedan hacer el cierre de las mismas. La evidencia de dicho cierre deberá ser notificada a la DGAST y guardados los registros correspondientes en casi de que sean requerido por algún proceso de auditoria o investigación de incidente de seguridad.

H. DESARROLLO DE SOFTWARE

1. La Dirección General Adjunta de Arquitectura y Diseño de Tecnologías de Información (DGAADTI) a través de sus Direcciones de Arquitectura Aplicativa (DAA) y Arquitectura de Sistemas (DAS) será las únicas áreas al interior de la Secretaría que podrán desarrollar software.

2. El desarrollo de software deberá llevarse a cabo en apego a mejores prácticas de programación que garanticen que la codificación se hace bajo estándares de seguridad adecuados.

3. La DGAADTI será la responsable de garantizar que los programas que son puestos en producción en equipos a cargo de la DGTII, hayan sido revisado en búsqueda de

vulnerabilidades de código que pudieran ser explotadas de manera maliciosa y pudiesen afectar la integridad o confidencialidad de la información.

I. REPALDOS DE INFORMACIÓN

1. La DGAOTI será la responsable de llevar a cabo el respaldo de toda la información contenida en los equipos de procesamiento central a cargo de la DGTII.

2. Los respaldos deberán hacerse con la periodicidad necesaria que minimice en medida de lo posible la posibilidad de pérdida de información en caso de alguna falla o caso fortuito.

3. Los respaldos deberán resguardarse en duplicado manteniendo un juego en el centro de datos y otro fuera del mismo para minimizar la posibilidad de pérdida de información en caso de un sismo.

4. En cuanto a los equipos personales que tengan catalogada información confidencial y/o estratégica, la DGAOTI será la responsable de llevar a cabo el respaldo de toda la información contenida en los mismos a solicitud expresa de los usuarios que lo consideren necesario. Esta información no podrá ser resguardada por la DGAOTI por periodos de más de un año.

J. BORRADO DE INFORMACIÓN

1. La DGAST será responsable de proveer el software necesario para llevar a cabo el borrado seguro de información de la infraestructura física cuando ésta deje de operar o sea retirada del Centro de Datos, en cumplimiento a lo establecido en los lineamientos generales aplicables.

2. La DGAOTI será la responsable de ejecutar el borrado seguro de los equipos con el software proporcionado por la DGAST y guardar los certificados que demuestren el proceso, mismos que podrán ser requeridos en caso de auditoría o investigación por incidente de seguridad.

Director General de Tecnologías de Información e Innovación.
Diciembre 2015