POLÍTICAS DE SEGURIDAD INFORMÁTICA

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (DGTIC)

SECRETARÍA DE LA FUNCIÓN PÚBLICA (SFP) DE LA PRESIDENCIA DE LA REPÚBLICA DEL PARAGUAY

Tabla de contenido

Presentación de Políticas de Seguridad Informática

Introducción

Con los avances alcanzados en materia de gobierno electrónico para la mejora de la eficiencia, la eficacia, la transparencia en la gestión pública y la promoción de la participación ciudadana, las tecnologías de la Información y la Comunicación (TIC) se han convertido en pilar fundamental de la gestión pública, por lo que la seguridad informática ha adquirido gran importancia, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes como la red internet, ha abierto nuevos horizontes a las instituciones para mejorar sus servicios y poder explorar más opciones de automatizar y facilitar la vida a los ciudadanos a través del desarrollo del gobierno electrónico, lo cual lógicamente, ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Para minimizar el impacto de eventuales ataques a la plataforma tecnológica de TIC se han desarrollado muchas documentaciones y directrices que orientan en el uso adecuado de las TIC y recomendaciones para obtener el mayor provecho de estas ventajas y evitar el uso indebido de las mismas, que puede ocasionar interrupciones de servicios, daños a los bienes y hasta paralizar el funcionamiento de la institución.

Tomando en consideración estas amenazas, el establecimiento de las políticas de seguridad informática constituyen una herramienta institucional para hacer conciencia a los funcionarios de la institución sobre la importancia y la sensibilidad de la información y servicios críticos que permiten a la institución crecer y mantenerse como institución líder en innovación. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la institución, conocimientos técnicos para detectar fallas y debilidades y constancia para renovar y actualizar las políticas de seguridad en función de los constantes avances tecnológicos ante los cuales, las instituciones deben poder enfrentarlos.

Definición de políticas de seguridad informática

La definición de políticas de seguridad informática, consisten en elaborar un canal de comunicación documentado por el cual se comunica a los usuarios, sobre las políticas de seguridad, en relación a los equipos y sistemas informáticos que soportan los servicios institucionales. En síntesis, son una declaración formal de las normas que los usuarios deben respetar a fin de acceder a los bienes de tecnología e información.

A través de las políticas de seguridad informática, se transmite cuáles son los bienes y servicios que se desean proteger y el porqué de esa necesidad. Cada política de seguridad es una invitación a cada usuario a reconocer cuán importante son los sistemas y las informaciones que constituyen activos intangibles de la institución, la razón de ser de nuestra institución. Esta documentación, no debe considerarse como un manual técnico informático ni una reglamentación sancionatoria de las conductas de los funcionarios. Más bien, las políticas de seguridad informática deben influenciar en la conciencia del funcionario para el uso adecuado de los recursos y servicios informáticos.

Componentes de una Política de Seguridad Informática (PSI)

Teniendo en cuenta que una política de seguridad informática debe alinear las medidas que se toman en relación a la seguridad, es fundamental que todos los funcionarios estén con la predisposición para lograr una visión consensuada de lo que se considera importante proteger.

Las PSI deben contemplar los siguientes componentes:

- El alcance de la política, incluyendo la infraestructura, los sistemas informáticos y a los funcionarios a quienes se les aplica la política establecida.
- Los objetivos de la política y una clara descripción de los componentes involucrados en la definición de cada política.
- El establecimiento claro de las responsabilidades para cada uno de los recursos y servicios informáticos y que afecta a todos los niveles jerárquicos de la institución.
- La definición de sanciones por violaciones de las políticas de seguridad establecida.
- La responsabilidad de los usuarios de los sistemas en relación a la información obtenida de los sistemas.

POLÍTICAS DE SEGURIDAD INFORMÁTICA (PSI)

PSI -1 Backup's de Base de Datos

Descripción

Backup de respaldo de las bases de datos institucionales para continuidad del servicio.

Objetivo

Mantener un backup actualizado de contingencia de todas las bases de datos institucionales en sitio alternativo.

Procedimiento

1) Mantenimiento de la configuración de la tarea programada (CRON) que genera el backup de cada una de las bases de datos del entorno de producción.
2) Verificación del alojamiento exitoso del archivo de backup en sitio alternativo, que el proceso de la noche haya finalizado satisfactoriamente.
3) En caso de resultado fallido del procedimiento 2), previsión del traslado físico del backup.

En todos los casos se debe realizar la prueba de restauración del backup cada 48 horas para la verificación de la validez del backup.

El responsable

1. De la ejecución del proceso de backup, el Jefe del Departamento de Soporte Técnico (Interno 2038)
2. De las pruebas de restauración del backup, el Jefe del Departamento de Desarrollo TIC's. (Interno 2034)

El acceso a los archivos de backup's estará restringido y se permitirá únicamente a los dos Jefes de Departamentos mencionados.

PSI – 2 Generación de backup's de archivos de usuarios

Descripción

Backup de respaldo de información sensible generado por los funcionarios en sus respectivos equipos de cómputo.

Objetivo

Mantener un backup actualizado de contingencia de la información relevante existente en documentos de texto, planillas electrónicas, diapositivas de presentaciones, materiales audiovisuales y cualquier otro tipo de trabajo producido para el cumplimiento de sus funciones.

Procedimiento

1) Los Directores Generales y Directores cada una de las Direcciones de la Secretaría de la Función Pública decidirán cuáles son los productos relevantes generados en el área que deben ser respaldados en el servidor de archivos.
2) Los archivos a ser guardados en el servidor de archivos no deben incluir información personal del usuario, solamente la información producida para el cumplimiento de sus funciones en la SFP.
3) Cada usuario deberá mantener en su equipo de cómputo la información original, siendo una copia de contingencia la guardada en el servidor de archivos.
4) El usuario es el responsable de la información guardada en el servidor de archivos.
5) La ausencia de la copia de respaldo en el servidor de archivos, será responsabilidad del usuario.
6) La violación del procedimiento 2) será notificada al superior del área por primera vez, la reincidencia será comunicada a la MAI.
7) El Jefe del Departamento de Soporte Técnico está autorizado a realizar monitoreo periódico de los archivos guardados en el servidor de archivos.

El responsable

1. El usuario es el responsable de mantener la copia actualizada de sus datos relevantes en el servidor de archivos.
2. El monitoreo e Informe sobre la violación del procedimiento 2) estará a cargo únicamente para el Jefe de Soporte Técnico (Interno 2038).

PSI – 3 Seguridad perimetral o física

Descripción

Acceso físico al Data center y seguridad de los equipos de cómputo asignados a los usuarios.

Objetivo

Mantener la seguridad física del data center, todo lo referido a los equipos informáticos y equipamiento de red, todo con el fin de mitigar eventuales ataques internos o externos.

Procedimiento

1) La restricción del acceso físico al área del data center por parte de personas ajenas al Departamento de Soporte Técnico. Se encuentra vigente la Resolución SFP Nº 278/2014 por la cual se Reglamenta el acceso y la permanencia de Personas (Art.3°).

2) Prohibición de abrir las PCs y/o manipular por parte del usuario, sólo está autorizado el personal de soporte técnico.

   La violación del procedimiento 2) será notificada al superior del área por primera vez, la reincidencia será comunicada a la MAI.

3) Si por razones de servicio, es necesario prestar equipos informáticos (computadoras portátiles tipo notebook) u otro tipo de equipo informático para ser utilizado en alguna presentación o evento, es obligatorio registrar en el libro de entrada/salida de equipos informáticos, fecha de retiro, fecha de devolución, firma y aclaración de nombres y apellidos.

4) El mantenimiento de los equipos servidores se efectuará de una manera programada y si fuese posible fuera del horario laboral ordinario, previa comunicación por correo electrónico a todos los funcionarios de la institución y si fuese necesario también a través de la página web institucional sobre la interrupción del servicio de tecnología.

El responsable

1. El monitoreo e informe al superior sobre la violación de los procedimientos del 1) y 2) estará a cargo del Jefe del Departamento de Soporte Técnico (Interno 2038).

PSI – 4 Seguridad de la red interna (LAN)

Descripción

Acceso a la red interna de la SFP.

Objetivo

Mantener la seguridad de la red interna de la SFP con el fin de minimizar los riesgos de ataques internos y/o externos.

Procedimiento

1) Actualización de la configuración del dispositivo enrutador o cortafuego con una correcta activación de la licencia y de los servicios de filtrado de Contenido Web, Antivirus, Anti Spam y registro en el Sitio web de Soporte del enrutador, para luego activarlos, crear los perfiles de Antivirus, crear los perfiles de Filtrado Web, crear los perfiles de Anti Spam, aplicar políticas de cortafuego relacionando los Perfiles de Protección con las diferentes políticas.

2) Habilitar credenciales de acceso a la red interna previa comunicación desde la Dirección de Gestión de Personas y el formulario de creación de usuarios correspondiente.

El responsable

La aplicación del procedimiento 1) y 2) está a cargo del Jefe del Departamento de Soporte Técnico (Interno 2038).

PSI – 5 Seguridad del correo electrónico

Descripción

Disponibilidad del correo electrónico institucional de la SFP.

Objetivo

Mantener la seguridad del correo electrónico institucional, libre de virus y demás códigos maliciosos para mantener operativo el servicio de correo electrónico y asimismo, para salvaguardar la reputación institucional.

Procedimiento

1) Mantenimiento del servidor de correo Zimbra configurado correctamente en cuanto a medidas de seguridad.

2) Administración de las cuentas de correo electrónico institucional en base al formulario de Alta, Baja o Modificación de usuarios y la configuración del software cliente de correo electrónico en las estaciones de trabajo.

3) Emitir alertas y tips de seguridad para los usuarios del correo electrónico institucional sobre los correos electrónicos entrantes maliciosos de suplantación de identidad (phishing) por los cuales solicitan sus credenciales de acceso (usuario y contraseña).

4) **Comunicación periódica a los usuarios del correo institucional "de que en ningún caso la DGTIC solicitará que ingresen su usuario ni contraseña por correo electrónico. Los correos que solicitan usuario** y contraseña tienen intenciones maliciosas, NO RESPONDA.

El responsable

La aplicación del procedimiento 1), 2) y 3) está a cargo del Jefe del Departamento de Soporte Técnico (Interno 2038).

PSI – 6 Seguridad de Internet

Descripción

Acceso prudente al servicio de Internet de la SFP.

Objetivo

El uso racional del ancho de banda de internet contratado y para fines exclusivamente institucionales para el desempeño de sus funciones.

Procedimiento

1) Administración del acceso a Internet por parte de los usuarios de la red interna, aplicando las restricciones de acuerdo a las funciones que desempeña cada funcionario.
2) Configurar los dispositivos de accesos inalámbricos.
3) Emitir alertas y tips de seguridad para los usuarios de Internet.

El responsable

La aplicación del procedimiento 1), 2) y 3) está a cargo del Jefe del Departamento de Soporte Técnico (Interno 2038).

PSI – 7 Seguridad del Servidor de Archivos

Descripción

Acceso al servidor de archivos de la SFP (la memoria institucional)

Objetivo

Asegurar los archivos producidos en la SFP consistentes en documentos fuentes, documentos portables (Pdf), planillas electrónicas, presentaciones, materiales audiovisuales, imágenes, entre otros documentos.

Procedimiento

1) Administración del Servidor de Archivos en cuanto a creación de carpetas y otorgamiento de privilegios adecuados para cada usuario sobre las carpetas, en base al Formulario de Alta, Baja o Modificación de usuarios.
2) Creación de usuarios del Servidor de Archivos en base al formulario de Alta, Baja y Modificación de usuarios.

El responsable

La aplicación del procedimiento 1) y 2) está a cargo del Jefe del Departamento de Soporte Técnico (Interno 2038).

PSI – 8 Seguridad del Circuito Cerrado de TV (CCTV)

Descripción

Circuito Cerrado de TV, forma parte de la seguridad perimetral (PSI - 3)

Objetivo

Registrar los movimientos de personas en las áreas monitoreadas

Procedimiento

1) Monitoreo sobre el correcto funcionamiento de las cámaras del CCTV
2) Monitoreo de la computadora en la cual se registran las imágenes.

El responsable

La aplicación del procedimiento 1) y 2) está a cargo de la Dirección de Soporte y Mantenimiento (Interno 2035).

PSI – 9 Seguridad lógica

Descripción

Velar por la aplicación correcta de las políticas de contraseñas en los sistemas.

Objetivo

La aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Procedimiento

1) Aplicación de las políticas de contraseñas al momento del diseño de los sistemas.
2) Administración de usuarios (Altas, Bajas y Modificaciones) de los sistemas informáticos con la aplicación de formularios habilitados para el efecto y los documentos requeridos para alta, baja, modificación de usuarios y asignación de roles.

El responsable

La aplicación del procedimiento 1) estará a cargo de la Jefatura del Departamento de Desarrollo TIC's (Interno 2034).
La aplicación del procedimiento 2) estará a cargo de la Jefatura de Atención a Usuarios (Interno 2050).

PSI – 10 Delitos informáticos

Descripción

Respeto sobre los Derechos de Autor y atención contra Delitos Informáticos.

Objetivo

Velar por el cumplimiento de las Leyes sobre los Derechos de Autor y contra los Delitos Informáticos. Estableciendo medidas para evitar la reproducción, instalación de programas informáticos no autorizados y entrega de códigos fuentes sin la debida autorización institucional por Resolución de la MAI.

Procedimiento

1) Restricción para los usuarios de equipos de cómputo, a instalar software de aplicación fuera de los autorizados por la SFP.
2) Restricción de copiar o comercializar ningún software propiedad de la SFP.
3) Restricción de distribuir o comercializar cualquier dato o información a los que tenga acceso en el ejercicio de sus funciones
4) Restricción de alterar o borrar códigos fuentes o de cualquier otro modo que ocasione daño en las aplicaciones informáticas de la SFP.

La violación de estos procedimientos 1), 2), 3) y 4) serán causales de acciones legales.

El responsable

El monitoreo sobre el respeto a estas restricciones estará a cargo de la Jefatura del Departamento de Soporte Técnico. En caso de detectarse la violación de cualquiera de estos procedimientos informará al superior inmediato (Interno 2038).

TETÃ REMBIJOKUÁI SÃMBYHYHA SECRETARÍA DE LA FUNCIÓN PÚBLICA
MARIA LORENA REGUERA CUBILLA
2018.05.09 16:09:58 -04'00'

TETÃ REMBIJOKUÁI SÃMBYHYHA SECRETARÍA DE LA FUNCIÓN PÚBLICA
HUMBERTO RUBEN PERALTA BEAUFORT
2018.05.09 16:03:35 -04'00'