

SENADO DE PUERTO RICO

RECIBIDO SECRETARIA
SENADO DE P.R.
2010 AUG 11 PM 2:48



Hon. Thomas Rivera Schatz
Presidente del Senado

ORDEN ADMINISTRATIVA – 10-66

**A: SEÑORES, SEÑORAS SENADORES, DIRECTORES DE OFICINA,
FUNCIONARIOS Y EMPLEADOS ADMINISTRATIVOS DEL SENADO**

ASUNTO: CREACIÓN DE LA OFICINA DE TECNOLOGÍA E INFORMÁTICA

Artículo I. Creación

Esta Orden Administrativa crea la Oficina de Tecnología e Informática del Senado de Puerto Rico y define sus funciones. Esta Oficina estará adscrita a la Oficina del Presidente del Senado.

Artículo II. Base Legal

Esta Orden Administrativa se promulga al amparo de la Sección 9 del Artículo III de la Constitución del Estado Libre Asociado de Puerto Rico; la Sección 6 del Reglamento del Senado, Resolución del Senado 27, aprobada el 12 de enero de 2009; así como la Resolución del Senado 28, aprobada el 12 de enero de 2009.

Artículo III. Funciones

La Oficina de Tecnología e Informática administrará los recursos, equipos y materiales que sirven las necesidades del Senado de Puerto Rico en lo que respecta al procesamiento electrónico de datos y dará apoyo a todas las oficinas administrativas y legislativas del Senado de Puerto Rico.

Artículo IV. Vigencia

Esta Orden Administrativa tendrá vigencia inmediata y el original deberá ser radicada en la Secretaría y copia de la misma distribuida a los legisladores y oficiales correspondientes.

En San Juan, Puerto Rico, hoy 11 de agosto de 2010.



THOMAS RIVERA SCHATZ
Presidente

RECIBIDO SECRETARIA
SENADO DE P.R.

2010 AUG 10 AM 10: 08



Manual de Normas y Procedimientos

Senado de Puerto Rico
Oficina de Tecnología e Informática

PREPARADO POR: OTI
VERSIÓN: 1.1

A handwritten signature in blue ink, consisting of several loops and flourishes, is located in the lower right quadrant of the page.

Tabla de Contenido

Introducción	1
Objetivo	1
Seguridad	1
Prevención de Daños.....	2
Acceso Físico.....	2
Procedimiento para Administración de Usuarios de la Oficina de Tecnología e Informática	3
Propósito.....	3
Alcance	3
Política	4
Descripción del Procedimiento	4
Documentación de Uso no Autorizado del Sistema	6
Glosario.....	7
Procedimiento para Solicitud de Equipo y Programas de Computadora.....	8
Propósito.....	8
Alcance	8
Política	8
Descripción del Procedimiento	8
Procedimiento para Instalación de Software y Cumplimiento con Leyes de Derecho de Autor (Copyright)	9
Propósito.....	9
Alcance	9
Política	9
Descripción del Procedimiento	10
Procedimiento para Reportar Averías, Solicitar Apoyo Técnico y Establecer Estándares para el Uso del Hardware y Software.....	10
Propósito.....	10
Alcance	10
Política	11
Descripción del Procedimiento	11
Procedimiento para Manejo de Correo Electrónico, Acceso a Internet y Prevención de Virus.....	12
Propósito.....	12

Alcance	12
Política para el correo electrónico	13
Descripción del procedimiento para el correo electrónico	13
Política para virus	14
Descripción del procedimiento para virus	14
Política para el uso de Internet	15
Procedimientos a Efectuarse Diariamente en la Oficina de Tecnología e Informática	15
Propósito.....	15
Alcance	15
Política	16
Descripción de los Sistemas Instalados	16
Descripción del Procedimiento	16
Guías de resguardo “Backup” de Información.....	16
Propósito.....	16
Alcance	16
Política	16
Descripción del Procedimiento	17
Responsable.....	18
Glosario.....	18
PROCEDIMIENTO PARA COMUNICACIONES Y CONEXIONES EXTERNAS.....	18
Propósito.....	18
Alcance	18
Política	18
Descripción del Procedimiento	19
Responsabilidad	19
Glosario.....	20
PROCEDIMIENTO PARA ATENDER CAÍDAS DEL SISTEMA	20
Propósito.....	20
Alcance	20
Política	20
Descripción del Procedimiento	20
Evaluación de la Caída.....	20

PROCEDIMIENTOS PARA LA EVALUACIÓN, ADQUISICIÓN, DESARROLLO, MODIFICACIÓN E IMPLEMENTACIÓN DE PROGRAMAS Y APLICACIONES	22
Propósito.....	22
Alcance	22
Política	22
Proceso de Pre Implantación.....	22
Proceso de Implementación.....	23
Proceso de Post-Implementación.....	23
Proceso de Control de Cambios	23
Procedimiento.....	24
Pre Implementación	24
Implementación.....	24
Post-Implementación	25
Control de Cambios.....	25

Introducción

El propósito de este Reglamento es establecer las normas que regirán el uso oficial de los equipos, materiales y recursos humanos que integran la Oficina de Tecnología e Informática (OTI) del Senado de Puerto Rico.

La OTI se establece con el propósito de administrar los recursos humanos, equipos y materiales que sirven las necesidades del Senado de Puerto Rico en lo que respecta al procesamiento electrónico de datos, así como para dar apoyo a todas las oficinas administrativas y legislativas del Cuerpo.

Como parte del proceso de diseñar e implementar el sistema de control interno, la Oficina de Tecnología e Informática (OTI) se ha dado a la tarea de preparar en forma integral la descripción de los procedimientos a seguir por el personal de la Oficina de Tecnología e Informática, los cuales constituyen el pilar para poder desarrollar adecuadamente las actividades, generando información útil y necesaria, estableciendo medidas de seguridad, control y autocontrol y objetivos que participen en el cumplimiento con la función del sistema.

La OTI tendrá a su cargo brindar el mejor servicio a todas las oficinas y empleados en el Senado de Puerto Rico. El servicio será de calidad y orientación para el mejor desempeño de los Sistemas de Información.

Objetivo

Con la preparación de este manual se tiene como objetivo el establecer las guías y estándares para el uso y funcionamiento de los sistemas de información del Senado de Puerto Rico. De manera específica se persigue:

- A) Establecer los mecanismos esenciales para el desempeño organizacional de la OTI.
- B) Proveer un servicio de excelencia a todas las oficinas administrativas y legislativas.

Este manual estará complementado con el Plan de Contingencia que se ha desarrollado para atender situaciones donde no se pueda acceder al sistema.

Seguridad

El acceso a los Sistemas debe ser apropiadamente autorizado y estará garantizado solamente para atender sus responsabilidades como empleados del Senado de Puerto Rico. La OTI retiene los derechos exclusivos de usar todos los equipos de computación y la información que reside en ellos y que está a cargo de salvaguardar solamente todos los datos que residen en nuestros Servidores.

Con el fin de proveer la seguridad de los datos, la OTI implantará controles dirigidos a mantener la integridad de los datos registrados en el sistema, estableciendo controles de acceso así como procesos de autenticación de usuarios y perfiles de acceso a la información según las funciones que desarrollen dentro del sistema. Asimismo establecerá los procesos de protección de información almacenada y su recuperación y se preparará un plan para la prevención de desastres.

La OTI utilizará software para el control de acceso a la red que incluya además de identificación de usuario, protección contra virus, cortafuegos (*firewall*) y sistemas de detección de intrusos.

La OTI mantendrá actualizado los inventarios de equipo de computación, periférico, de comunicaciones y software; hará monitoreo del uso de los mismos.

La OTI mantendrá actualizados los mapas de topología de la red y dará seguimiento al funcionamiento de la misma, identificando tiempos de espera anormales en la transmisión de datos y mejoras que puedan hacerse a la infraestructura para optimizar el uso de la misma.

La OTI se mantendrá actualizado respecto a la identificación de riesgos que puedan afectar la integridad del sistema y el uso de la información que maneja por parte de usuarios no autorizados.

Prevención de Daños

Para la protección de los equipos en las diferentes oficinas, la OTI instalará equipo para protección por los cambios de voltaje en el fluido eléctrico y/o baterías para garantizar que el equipo continúe funcionando después de cortes en la energía, el tiempo suficiente hasta ir a través del proceso normal de “*shutdown*” del sistema. La OTI cuenta con equipos de aire acondicionado, extintores de incendios y detectores de humo.

Acceso Físico

Para tener acceso al sistema se requiere que el usuario haga “*login*” en el sistema, para lo que debe tener su identificación de usuario “*User-Id*” y contraseña “*password*”, que la otorga la OTI mediante un formulario de petición donde se indica el propósito de uso y está firmada por el supervisor del área.

Está prohibido al usuario:

- 1) Compartir o prestar su clave de acceso al sistema. Si el usuario sospecha que alguien está usando su identificación, deberá solicitar inmediatamente a la OTI el cambio del mismo. El encargado de Infraestructura de la OTI deberá revisar con el usuario para verificar que se está cumpliendo con la política de privacidad de acceso al sistema. De continuar presentándose la situación con este usuario, podrá deshabilitar el acceso de ese usuario al sistema.

- 2) Los usuarios no deberán dejar las estaciones desatendidas mientras haya una sesión en progreso. Para asegurar la confidencialidad de la información, los usuarios deben dar “log off” al sistema cuando se vayan a retirar de la estación.
- 3) Cualquier computadora o programa (aplicación) que sea propiedad del Senado de Puerto Rico, y/o programas o paquetes de cómputo adquirido por el mismo en términos de compra, renta o licencia de uso, NO DEBE ser utilizado para propósito diferente a las operaciones del organismo mencionado.
- 4) Las computadoras personales conectadas a las computadoras centrales (Servidores) deberán cumplir con todos los procedimientos y políticas sobre seguridad de los datos aplicables a estos sistemas, incluyendo identificaciones de usuario y contraseñas.
- 5) El acceso físico a las computadoras personales deberá ser restringido y solo podrán utilizar los equipos, aquellos usuarios que hayan sido previamente autorizados por el área local.
- 6) Se restringirá el acceso de personal ajeno a la OTI y las compañías que dan apoyo a los sistemas instalados, a las áreas donde están ubicados los servidores.

Procedimiento para Administración de Usuarios de la Oficina de Tecnología e Informática

Propósito

Documentar el proceso de solicitud, análisis, aprobación e implementación de acceso lógico a los recursos del sistema.

Estandarizar la forma como se solicita el acceso de nuevos usuarios, las modificaciones de accesos a los recursos y la eliminación de cuentas de usuarios, de manera que se contemplen todos los posibles requerimientos de un usuario.

Crear los mecanismos mediante los cuales se logre integrar y coordinar la creación de usuarios en los diferentes componentes del sistema.

Disponer el que se documente en forma organizada un sistema eficiente para administrar los usuarios que operan en la red del Senado de Puerto Rico.

Alcance

El presente procedimiento será aplicado al control de acceso lógico a los siguientes componentes del ambiente informático:

- 1) Plataformas de procesamiento (sistemas operativos Windows)
- 2) Sistemas que procesan información
- 3) Información del sistema
- 4) Servicios de red (ejemplo: correo electrónico, Internet, impresoras, etc.)

Política

La administración de usuarios del dominio del Senado de Puerto Rico es responsabilidad del encargado de Sistemas de la Oficina de Tecnología e Informática. Las cuentas de las aplicaciones estarán a cargo de los líderes de las aplicaciones. Sus responsabilidades primarias son:

- 1) Conocer el documento y establecer las medidas necesarias para cumplir con lo establecido en este procedimiento.
- 2) Dar acceso a los usuarios conforme a las peticiones establecidas en el documento de solicitud de acceso.
- 3) Dar mantenimiento a las cuentas de los usuarios.

Para acceder al sistema de información del Senado de Puerto Rico todo usuario deberá tener una cuenta en el dominio de Senado, que lo autorice a utilizar los servicios de la red.

Para acceder a cada uno de los sistemas que hacen parte del sistema de información del Senado, cada usuario deberá tener una cuenta que le de acceso a aquellos componentes del sistema que vaya a utilizar según las labores que vaya a realizar en él.

Descripción del Procedimiento

1) Creación de nuevos usuarios

- a. Los funcionarios autorizados para solicitar la creación de usuarios serán los directores de cada oficina o los empleados designados mediante el formulario de “Personal Autorizado a Firmar el Formulario para la Creación, Renovación o Modificación de Cuentas en la Red Local y el Correo Electrónico y demás formularios de la Oficina de Tecnología e Informática”.
- b. Para la creación de nuevos usuarios se empleará la forma “Formulario de Acceso al Usuario a los Sistemas de Información del Senado”.
- c. La solicitud deberá ser complementada en todas sus partes, firmada por el director o designado de la oficina y enviada a la OTI mediante email o fax al 787-723-4860. Quien reciba la solicitud en el OTI, la circulará a los encargados de la creación de cuentas y de las aplicaciones para las que se esté solicitando acceso.
- d. El administrador del sistema será responsable de que se cree la cuenta del usuario en la red de Senado e informar el nombre de usuario (“*username*”) y contraseña (“*password*”) para el acceso a Windows.
- e. Los encargados de las aplicaciones para las que se esté solicitando acceso, informarán al usuario sus claves de acceso y le darán instrucciones de cómo hacer “*login*” en el sistema.

- f. En caso de ser un usuario con privilegios administrativos en la red del Senado, el responsable de llevar a cabo este procedimiento es el director de la Oficina de Tecnología e Informática mediante el formulario correspondiente. Una vez completados los formularios de acceso, se procederá a incluir el usuario al grupo de “*Domain Admins*”.

La contraseña es confidencial, de uso exclusivo del usuario, no podrá ser igual al nombre de usuario y no debe “**prestarse**” a otros usuarios.

Si se presenta un problema o anomalía durante el proceso acceder al sistema (“*login*”), deberá comunicarse con la OTI, extensión 3259.

2) **Modificación de un usuario en el sistema.**

Los directores o encargados de las oficinas serán responsables de informar al Administrador de Sistemas de la OTI cualquier modificación que sea necesaria hacer en el perfil de un usuario.

Aplicarán los mismos pasos que en el caso de creación de usuarios, especificando en la hoja de solicitud que se trata de una modificación al perfil del usuario.

- a. Bloqueo de un usuario en el sistema

Cualquier cuenta de usuario que haga un uso indebido del sistema podrá ser bloqueada por el Administrador de Sistemas de la OTI.

- b. Eliminación o baja de un usuario en el sistema

Los directores o encargados de las oficinas serán responsables de informar al Administrador de Sistemas de la OTI cuando un empleado se desvincule del Senado de Puerto Rico. La baja de su cuenta se efectuará de la siguiente manera:

- a) El director o encargado que tenga a su cargo al usuario que se desvincula, deberá enviar la notificación mediante carta o correo electrónico con la información detallando si se trata de una “baja programada” o “baja inmediata”, lo firmará y lo remitirá al Administrador de Sistemas, Oficina de Tecnología e Informática del Senado de Puerto Rico, indicando que se trata de Cancelación de Acceso o Separación de Servicio.
- b) El Administrador de Sistemas deberá:
 - Verificar que el comunicado contiene toda la información requerida.
 - Proceder a eliminar los accesos correspondientes del usuario que se desvincula de su servicio.
 - Una vez el empleado culmine sus servicios, la Oficina de Recursos Humanos enviará un Informe sobre Empleados Separados del Servicio. El mismo será completado y enviado a la Oficina de Recursos Humanos indicando si el empleado *Adeuda* o *No Adeuda* equipo

y/o cuentas relacionados con la OTI o el Senado de Puerto Rico. La OTI retendrá copia de los informes.

Acceso al Sistema

- 1) La OTI se comunicará con el usuario informándole su identificación de usuario (*User-Id*) y contraseña (*password*).
- 2) Si el usuario olvida sus claves de acceso al sistema, se comunicará con la OTI para solicitar su identificación de usuario y que se le asigne un nuevo *password*.
- 3) De acuerdo con las disposiciones de la OTI, los *passwords* expiran cada cuarenta y cinco (45) días. El sistema le informará al usuario con catorce (14) días de anticipación que su *password* está por expirar y el usuario deberá cambiarlo, para evitar que el sistema le inhabilite la cuenta. Para cambiar la contraseña debe presionar la combinación de teclas CTRL+ALT+DEL y presionar “*Change Password*”. De necesitar ayuda, deberá solicitarla a la Oficina de Tecnología e Informática.
- 4) En las áreas donde una estación es utilizada por varios usuarios, cada usuario deberá hacer *login* cuando vaya a utilizar el equipo y tan pronto termine de entrar el registro o la transacción hacer *logout* para evitar que otro usuario use el sistema con su identificación. Este paso es importante para evitar que la estación quede bloqueada con la clave de un usuario que no esté disponible para acceder al sistema cuando se vaya a utilizar de nuevo el equipo.
- 5) Las estaciones deberán tener activados los *screensavers* autorizados por la OTI, de forma tal que cuando una estación permanezca desatendida por más de diez (10) minutos, el *screensaver* se active.
- 6) Cualquier usuario que sospeche que su identificación en el sistema ha sido comprometida o quiere cambiar su *password*, solicitará el cambio a la OTI.

Documentación de Uso no Autorizado del Sistema

Si alguien detecta el uso no autorizado del sistema deberá informarlo a la OTI.

Toda persona que tenga acceso al sistema tiene el derecho y la responsabilidad de reportar cualquier fuga en la confidencialidad de la información sin temor a represalias por hacerlo. Si alguien detecta una falla en el manejo intencional o inadvertido de la confidencialidad de la información deberá reportar el incidente en la siguiente forma:

- A) Hacer una descripción por escrito del incidente y reportarla a la OTI. Esta descripción deberá contener:
 1. Fecha y hora, dónde y cómo ocurrió la brecha en la seguridad de la información.

2. Quienes estuvieron involucrados en el incidente.
 3. Nombres de otras personas que fueron testigos.
- B) El encargado de Sistema de la OTI confirmará por escrito el recibo de la notificación del incidente y enviará el informe al Director de la Oficina de Tecnología e Informática. Este informe será revisado con los involucrados para determinar la precisión del mismo. Si de la investigación resultara que efectivamente se presentó una brecha en la confidencialidad de la información, harán las recomendaciones tendientes a que no vuelva a ocurrir esta situación.

Glosario

Dominio: Es un conjunto de computadoras conectadas en una red que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en dicha red. El equipo en el cual reside la administración de los usuarios se llama controlador de dominio y cuando queremos usar un ordenador de dicha red tenemos que poner un nombre de usuario y una contraseña para ser reconocidos por el controlador de dominio y poder usar los recursos compartidos de la red (acceso a Internet, impresoras, software, etc.).

Login: El momento de iniciar una sesión en el sistema. Conlleva dos pasos mediante los cuales el sistema autentica que al usuario se le puede dar acceso al sistema:

→ El digitar una identificación de usuario.

→ El entrar una contraseña.

Logout: Es el momento en que se termina la sesión para ese usuario. En Windows seleccionando del menú de Start, Logoff.

Perfil: Asignación de acceso a aplicaciones de acuerdo al rol de trabajo del funcionario, debidamente aprobado por el supervisor del área y por la OTI.

Usuarios: Son todos los funcionarios que hacen uso de los sistemas o servicios tecnológicos, que proporciona la OTI.

User-Id: Identificación de usuario. Combinación de caracteres alfanuméricos que permiten identificar al usuario para el ingreso a un determinado sistema.

Password: es una palabra que se utiliza para acceder a datos restringidos de un sistema. Mientras que las contraseñas crean una seguridad contra los usuarios no autorizados, el sistema de seguridad sólo puede confirmar que la contraseña es válida, y no si el usuario está autorizado a utilizar esa contraseña.

Procedimiento para Solicitud de Equipo y Programas de Computadora

Propósito

Documentar el proceso de solicitud de los equipos de sistemas y programas de computadora.

Alcance

Este procedimiento aplica a todas las solicitudes de adquisición de equipos (hardware) y programas (software) para cualquier oficina o empleado del Senado de Puerto Rico que así lo necesite.

Política

Toda solicitud de utilización, adquisición y/o contratación de bienes y servicios informáticos debe ser solicitada exponiendo su justificación a la Oficina de Tecnología e Informática.

El usuario responsable del equipo de cómputo deberá mantener bajo su custodia el material que se le entregue para el funcionamiento del sistema.

El usuario responsable del equipo de cómputo deberá informar a la OTI y a la Oficina de Propiedad en caso de que se realice alguna transferencia del mismo, a fin de mantener el inventario de equipo actualizado para efectos de mantenimiento correctivo y preventivo.

Ningún empleado de la OTI deberá remover o transferir equipo alguno. Todo movimiento deberá ser autorizado, coordinado y ejecutado por la Oficina de Propiedad, quien deberá informar a la OTI para la conexión a la red o cualquier dificultad que se les presente.

Para dar de baja equipo de cómputo el responsable del equipo debe solicitar la baja a la OTI.

Queda prohibido que los usuarios agreguen o remuevan componentes tanto de software como de hardware de los equipos de cómputo. En caso de requerirse algún cambio este debe solicitarse a la OTI.

La OTI se reserva el derecho a monitorear el uso de los recursos y servicios informáticos.

La configuración de los equipos realizada por la OTI no deberá ser modificada por los usuarios.

La OTI es la única autorizada para configurar equipos para acceso a la red o a Internet.

Descripción del Procedimiento

- A) En los casos de solicitud de equipos de computadoras o programas, el supervisor del área se comunicará con la OTI para exponer la solicitud y conocer sobre la disponibilidad del mismo.

- B) La OTI estudiará la solicitud y de haber disponibilidad para el mismo, responderá al solicitante dentro de los próximos cinco (5) días laborables.
- C) De haber la disponibilidad para atender la solicitud, el supervisor del área enviará por escrito la solicitud, indicando el área y justificando el uso que se dará al equipo o software solicitado.
- D) Al ser adquirido el equipo y recibido por la Oficina de Propiedad, esta coordinará con la OTI para la configuración y conexión del equipo.
- E) La OTI actualizará el Inventario de Equipos y Programas con la nueva ubicación del equipo o programa.
- F) El director de la oficina al que se le entregue el equipo será custodio y responsable por el material que se le entregue.
- G) La Oficina de Tecnología e Informática incluirá dentro del inventario de equipo y software el bien recibido y la procedencia del mismo.
- H) Si por necesidades del servicio fuera necesario mover el equipo, este movimiento será solicitado mediante una llamada de servicio a la OTI, quienes procederán a efectuar el mismo.
- I) La OTI hará rondas no anunciadas por las diferentes estaciones para verificar que se está cumpliendo con lo dispuesto en este procedimiento.

Procedimiento para Instalación de Software y Cumplimiento con Leyes de Derecho de Autor (Copyright)

Propósito

Reglamentar la instalación de programas de computadora y garantizar que la Oficina de Tecnología e Informática del Senado de Puerto Rico cumple con las normas de derechos de autor (Copyright).

Alcance

Este procedimiento aplica a todos los programas de computadora que se instalen en equipo de computación que sea propiedad de la Oficina de Tecnología e Informática.

Política

Solamente el personal de Sistemas podrá instalar programas de computadora en las computadoras de las distintas oficinas del Senado de Puerto Rico, y lo hará cumpliendo con las

leyes de derechos de autor (copyright), instalando solamente software para el cual cuente con las respectivas licencias para su uso.

Solamente el personal de Sistemas podrá cambiar la configuración de las computadoras. Cualquier usuario que necesite cambiar la configuración de su computadora para el desarrollo de sus labores, lo solicitará a la Oficina de Tecnología e Informática.

Está prohibido reproducir cualquier tipo de programa de cómputo o documentación relacionada, bien sea para uso en las Oficinas del Senado o en cualquier otro lugar, a menos de que la persona responsable de tal acción esté expresamente autorizada para hacerlo porque tiene la licencia.

La reproducción no autorizada de Programas de Cómputos puede ocasionar al Senado de Puerto Rico, responsabilidades civiles y penales, de acuerdo con la Ley Derechos de Autor (copyright).

Los empleados no pueden dar programas de Cómputo a terceros, incluyendo clientes, contratistas u otras personas ajenas al Senado de Puerto Rico.

Descripción del Procedimiento

- A) De ser necesaria la instalación de un programa el supervisor del área hará la solicitud por escrito a la Oficina de Tecnología e Informática.
- B) La Oficina de Tecnología e Informática estudiará la solicitud y de encontrarla justificada, si hay licencias disponibles para el programa, destacará a un técnico de sistemas para que haga la instalación correspondiente. Si el programa debe ser adquirido, seguirá el procedimiento para ese fin.
- C) La Oficina de Tecnología e Informática actualizará el inventario de programas instalados.
- D) La Oficina de Tecnología e Informática hará rondas no anunciadas para verificar los programas instalados en las computadoras. De encontrar software no autorizado instalado en las estaciones, procederá a removerlo y a informar por escrito al supervisor del área, sobre la infracción cometida.

Procedimiento para Reportar Averías, Solicitar Apoyo Técnico y Establecer Estándares para el Uso del Hardware y Software

Propósito

Establecer el procedimiento estándar para reportar averías en el sistema.

Alcance

Este procedimiento aplica a todos los usuarios del Senado de Puerto Rico.

Política

La Oficina de Tecnología e Informática mantendrá un sistema mediante el cual se pueda llevar una bitácora de las averías reportadas por oficinas, de forma tal que los técnicos de sistemas puedan tener acceso a ellas para consultar y documentar las situaciones atendidas.

Toda computadora estará conectada a un sistema regulador de voltaje, para prevenir daños por fluctuaciones en el fluido eléctrico.

Para prevenir sobrecargas que puedan alterar el normal funcionamiento de los equipos, se evitará conectar en la misma batería en la que se encuentra el equipo, periféricos de alto consumo de energía, tales como fotocopiadoras e impresoras laser.

Con el fin de prevenir accidentes, no se permitirá dejar cables que crucen por lugares en que transita el personal.

Toda instalación de cable estructurado, debe seguir los estándares de la industria y que han sido adquiridos por la Oficina de Tecnología e Informática. Por lo tanto, cualquier instalación nueva o cambio a la existente debe ser coordinado por la Oficina de Tecnología e Informática.

Se evitará el obstruir los orificios de ventilación de la CPU y el monitor, para evitar el calentamiento del mismo.

El cambio de ubicación de equipo de computación será realizado por la Oficina de Propiedad y coordinado por la Oficina de Tecnología e Informática.

Descripción del Procedimiento

- A) En caso de presentarse cualquier situación donde el usuario no pueda utilizar el sistema, deberá comunicarse con la Oficina de Tecnología e Informática, en el que personal de la OTI o Help Desk lo ayudará para la solución del problema.
- B) El Help desk deberá analizar la situación y de encontrar que no puede resolverla, se asignará una llamada de servicio y se enviara un técnico de sistemas para atender la solicitud. El técnico verificará la situación reportada y si es un problema con el equipo que no pueda resolver inmediatamente, se lo informará al usuario, indicándole el tiempo aproximado para la solución del mismo.
- C) Si la situación reportada tiene que ver con fallas en las aplicaciones, analizará la situación y si fuera necesario, procederá a reinstalar la aplicación.
- D) En los casos de problemas de comunicaciones donde se esté observando que ocurren con frecuencia, el técnico verificará el sistema de comunicaciones o los concentradores y hará pruebas y de no poder resolverla, escalará la situación al Director de la Oficina de Tecnología e Informática con el fin de que se contraten los servicios para resolver la situación.

- E) Si es un problema con el equipo que implica que debe ser enviado a reparación cubierta bajo la garantía, informará la situación a la Oficina de Tecnología e Informática, para que éste proceda a hacer el trámite para reportar el equipo a la compañía, e informará al usuario sobre la gestión realizada y tiempo aproximado de reparación. La Oficina de Tecnología e Informática deberá llevar un registro del equipo que se ha reportado para la reparación bajo garantía, y dará seguimiento a la reparación del mismo para asegurar que el usuario tenga de nuevo el equipo en el menor tiempo posible. El técnico de la Oficina de Tecnología e Informática deberá coordinar para que los servicios al usuario no se vean afectados mientras el equipo está en reparación.
- F) Al resolver una situación, el técnico de la Oficina de Tecnología e Informática le dará “reboot” al sistema y le pedirá al usuario que haga de nuevo “login” en el sistema y compruebe que la situación está resuelta, para que el usuario verifique que la situación reportada fue corregida. El técnico de la Oficina de Tecnología e Informática le pedirá al usuario que recree la situación que dio lugar a la llamada para verificar que fue corregida.
- G) El técnico de la Oficina de Tecnología e Informática que atienda la situación deberá llevar una bitácora en línea (preparar un reporte en línea) sobre la situación encontrada y como la resolvió.
- H) Tan pronto como un técnico de la Oficina de Tecnología e Informática atienda una llamada reportando averías con una computadora o equipo periférico, deberá analizar el historial del equipo y contar con información que le ayude a hacer un mejor diagnóstico de la situación y como resolverla.

Procedimiento para Manejo de Correo Electrónico, Acceso a Internet y Prevención de Virus

Propósito

Establecer las políticas y procedimientos para el manejo adecuado del correo electrónico, el acceso a internet y la prevención de virus para los usuarios del Senado de Puerto Rico.

Alcance

Este procedimiento aplica a todos los usuarios del Senado de Puerto Rico.

Política para el manejo del correo electrónico

El Reglamento de la Oficina de Tecnología e Informática establece que el correo electrónico es un mecanismo de comunicación para atender asuntos oficiales, directamente relacionados con la función pública, por lo que no se utilizará para asuntos de índole personal, privado o lucrativo.

Descripción del procedimiento para el manejo del correo electrónico

- A) Se prohíbe el uso del correo electrónico para uso personal. Se entiende por “uso personal”, sin que se entienda como una limitación, a: cartas, pensamientos, recetas, peticiones, recolectas, anuncios, propaganda comercial de eventos, artículos o propiedad para la venta o alquiler, que resulte en beneficio personal.
- B) Queda prohibido el uso del correo electrónico para actividades como: mensajes en cadena, mensajes raciales, obscenos, pornográficos, sugestivos o amenazas, distribución de mensajes comerciales, la propagación de “virus”, la presentación de mensajes a nombre de otra persona, real o ficticia, mensajes anónimos, mensajes de contenido libeloso o difamatorio, entre otros. El Senado de Puerto Rico no será responsable por la transmisión de esos mensajes.
- C) Se dispone que los usuarios del sistema de correo electrónico del Senado de Puerto Rico prestarán particular atención y cuidado al enviar sus mensajes a grandes audiencias y evitarán repetir los mismos “a manera de recordatorio”. La práctica correcta del envío de mensajes debe limitar el envío de los mismos al grupo de personas más pequeño posible. Únicamente en situaciones extraordinarias los administradores del sistema, serán los autorizados para enviar mensajes oficiales a grandes audiencias.
- D) Los usuarios del sistema tienen que asegurarse que al enviar contestaciones a los mensajes, dirijan las mismas a las personas deseadas y no a un grupo de personas.
- E) Cada usuario es responsable por la confidencialidad y seguridad de su contraseña (“password”).
- F) Está prohibido acceder a otra cuenta o computadora con una contraseña ajena, así como acceder a documentos que se encuentran en los archivos del correo electrónico de dicho usuario. Dicha acción constituye, además, una violación al “Federal Electronic Communications Privacy Act”, según enmendada, 18 U.S.C. sec 2510.
- G) El acceso no autorizado a información confidencial senatorial será atendido a tono con las disposiciones del Senado de Puerto Rico

- H) Se prohíbe la interceptación o acceso a correspondencia electrónica de carácter confidencial y la remisión de la misma a un tercero sin la autorización del remitente. Se entiende por comunicación confidencial cualquier mensaje de esta naturaleza entre remitente y destinatario, dentro de sus funciones en el Senado. Sin embargo, existen circunstancias específicas, mediante las cuales el Senado, a través de los administradores del sistema, pueden acceder a dichos archivos electrónicos para salvaguardar la integridad del sistema de correo electrónico y asegurar el cumplimiento de las leyes y normas aplicables.
- I) El Senado no tiene como política operacional, la inspección de la correspondencia electrónica, por lo que los administradores del sistema tienen que proteger la confidencialidad de los documentos y comunicaciones enviadas a través del correo electrónico del Senado de Puerto Rico. Cualquier inspección de dichos archivos, o cualquier acción basada en dicha inspección, deberá estar regida por las disposiciones establecidas en este Reglamento.
- J) Nunca envíe o transfiera mensajes electrónicos, sin permiso de la persona que originalmente los envía. Estos mensajes están protegidos por las leyes de "Copyright", por lo que no se pueden plagiar mensajes.
- K) El correo electrónico no puede ser utilizado para violar o incitar a la violación de las leyes y reglamentos estatales y federales, así como normas o políticas del Senado de Puerto Rico referentes al hostigamiento sexual o al discrimen.

Política para la prevención de virus

Los virus informáticos son pequeños programas diseñados intencionalmente para propagarse de un equipo a otro y para interferir en el funcionamiento del mismo sin el conocimiento o el permiso del usuario. Este programa ataca a los sistemas y se replica a sí mismo para continuar su esparcimiento.

Hay varios tipos de virus. Los más peligrosos son los que atacan cambiando la configuración de la computadora en forma que puede incluso llegar a dañarla permanentemente.

Los siguientes son los procedimientos recomendados para prevenir problemas con virus informáticos (para realizar algunos de ellos puede necesitar ayuda calificada):

Descripción del procedimiento para la prevención de virus

- A) Todo usuario debe tener un conocimiento básico de lo que son los virus informáticos y del programa antivirus instalado en su computadora.
- B) De necesitar utilizar un medio externo para acceder a información (CD, USB o drive externo), deberá analizarlo antes con el antivirus, para asegurarse que está libre de virus.
- C) Actualmente, el correo electrónico es el mecanismo más común de transporte de virus informáticos. Por esta razón;

1. Está prohibido abrir archivos extraños o macros anejos a los mensajes de correo electrónico que lleguen de un origen desconocido, sospechoso o poco confiable. Estos mensajes se deberán borrar inmediatamente, sin abrirlos; y luego borrarlos de la carpeta de borrados “Deleted Items” de su programa de consulta de correo Outlook. Además, deberá desactivar el panel de vista previa “Preview pane” para evitar que sus mensajes sean abiertos automáticamente.
2. Todos los mensajes tipo “spam” (correos de publicidad no solicitados y distribuidos a muchos destinatarios), cadenas (correos cuyo contenido invita a replicarlo varias veces a otras personas), y cualquier otro correo que no esté relacionado con las actividades propias de su trabajo deberán ser borrados.
3. Los técnicos de sistema configurarán las cuentas de correo electrónico de (Microsoft Outlook) para mostrar y bloquear extensiones de archivos anexos a los mensajes de correo con alta probabilidad de transportar virus, tales como los que traen anejos "attachments" con extensiones como .exe, .com, .pif, .scr y .bat.
4. Los usuarios deberán depurar su buzón “Inbox” y no dejar correos por largo tiempo para evitar llegar al límite de su cuota.
5. Al usar las cuentas de correo electrónico del Senado de Puerto Ricos, los usuarios usarán un lenguaje apropiado en sus comunicaciones.

Política para el uso de Internet

El acceso de un usuario a Internet debe solicitarlo el supervisor del área por medio del Formulario de Acceso al Sistema del Senado de Puerto Rico.

Para el uso de Internet aplicará la misma política de uso del recurso que para el correo electrónico y restricciones de uso de sistemas establecido por el Reglamento de la Oficina de Tecnología e Informática en el sentido que se permitirá solamente para propósitos oficiales.

Procedimientos a Efectuarse Diariamente en la Oficina de Tecnología e Informática

Propósito

Establecer los controles que deberán ejercerse diariamente en la OTI, con miras a que haya un monitoreo constante que minimice los problemas en la operación de los sistemas en el Senado de Puerto Rico.

Alcance

Este procedimiento aplica a los empleados de la OTI así asignados por el Director de la Oficina de Tecnología e Informática.

Política

La OTI del Senado tendrá asignado técnicos de la Oficina de Tecnología e Informática y programadores en el horario regular de trabajo.

Descripción de los Sistemas Instalados

En la OTI del Senado están instaladas diferentes aplicaciones del servicio de Exchange en servidores ubicados dentro del cuarto de Cómputos de la Oficina de Tecnología e Informática del Senado de Puerto Rico.

Descripción del Procedimiento

El personal que esté asignado deberá verificar diariamente que:

- A) Los servers estén funcionales. Si algún server no está funcional, procederá a comunicarse con el encargado o con el Director de la oficina, para coordinar los esfuerzos a fin de restablecer a la normalidad el sistema. También entrará en vigor el Plan de Contingencia.
- B) El “backup” corrió correctamente. De no ser así se comunicará con el encargado y el Director de la Oficina de Tecnología e Informática, para reportar la situación. Esta situación requiere especial atención y debe resolverse para asegurar que se haga un “backup” el mismo día que se detectó la falla.

Guías de resguardo “Backup” de Información

Propósito

Prevenir la pérdida de información. Este procedimiento es la base para el Plan de Contingencia en casos de desastres. Por lo tanto, debe contener todos los sistemas con las últimas modificaciones que se hayan efectuado, de tal manera que si ocurriera un desastre mayor, se pueda restaurar el sistema al estado en que estaba antes de ocurrir el desastre y debe cumplirse de manera sistemática

Alcance

Servidores de la red. No se hará “*backup*” de los discos de las computadoras. Los usuarios de las mismas serán responsables de tener su propio sistema de “*backup*” para el material que almacenen fuera de la red.

Política

Se establece como norma de la Oficina de Tecnología e Informática el que se efectúen diariamente los procedimientos de resguardo “*backup*” incremental en la OTI y se haga semanalmente uno total del sistema.

Al determinar los períodos de tiempo donde se efectuarán los procedimientos de resguardo se tendrá en cuenta aquellos en que menos se afecten las operaciones normales.

Los “*backup*” se guardarán en el área de bóveda donde el acceso es restringido y controlado.

Descripción del Procedimiento

- A) El proceso de “*backup*” contendrá los sistemas operativos y aplicaciones con las configuraciones especiales que se hayan hecho para adaptarlo a las necesidades específicas del sistema, las bases de datos de Exchange, las carpetas de los usuarios y aplicaciones compartidas.
- B) El sistema está configurado para que automáticamente corra un proceso de “Full Backup” en un período de tiempo que empieza todos los viernes a las 10 de la noche y hasta el sábado siguiente a las 4 de la mañana, que copia toda la información que está en los discos. Este Full Backup expira a las tres (3) semanas.
- C) El sistema está configurado para que diariamente corra un Differential Backup, en un período de tiempo que empieza a las 11 de la noche hasta las 6 de la mañana del día siguiente.
- D) El sistema Veritas backup efectúa backup en cintas que están en el cuarto de cómputos de la Oficina de Tecnología e Informática.
- E) Para efectos de retención de las cintas, se mantienen doce cintas mensuales, equivalentes a tres semanales.
- F) El encargado de dar seguimiento al proceso de backup verificará en pantalla que el proceso corrió exitosamente y de no ser así, investigará las razones por las cuales el proceso falló. Deberá volver a correr el proceso, asegurándose que terminó normalmente. De presentarse una situación que no pueda resolver procederá a consultarlo con el grupo de trabajo y resolver la situación en el menor tiempo posible.
- G) Se restringirá el acceso al sitio de almacenamiento de los backups y solamente el Director de la Oficina de Tecnología e Informática y a quienes éste designe tendrán acceso a los mismos.
- H) La Oficina de Tecnología e Informática periódicamente probará los procedimientos de backup y restore para asegurar que la data se puede recuperar de los backups.
- I) La Oficina de Tecnología e Informática llevará el registro de los medios utilizados para backup y el período durante el cual se mantendrán hasta volver a reutilizarlos.

Responsable

Administrador de Sistemas.

Glosario

Backup: Copia que se hace de los datos con el fin de tenerlos como respaldo en caso de que los originales se dañen o corrompan.

Restore: Es el proceso de copiar los datos desde el *backup* que se hizo previamente.

PROCEDIMIENTO PARA COMUNICACIONES Y CONEXIONES EXTERNAS

Propósito

El acceso remoto requiere controles adicionales de seguridad para mitigar el incremento en riesgos al permitir conectividad desde un ambiente externo al sistema del Senado.

Alcance

Esta política aplica a todas las conexiones remotas a los recursos de la OTI del Senado.

Política

El acceso remoto al sistema del Senado provee muchos beneficios. Permite al personal conectarse desde un ambiente remoto y provee la capacidad de teleconmutación. Sin embargo, el acceso remoto conlleva riesgos de intrusos y personas no autorizadas, así como la interceptación de datos que están siendo transferidos a través de la conexión remota. La conectividad directa a la Internet o a otras redes externas también carece de la protección de los cortafuegos (firewall) y otras protecciones que hay cuando se establece la conexión física. Para contrarrestar esto se deben entonces implantar medidas adicionales de seguridad para mitigar los riesgos que conlleva el acceso remoto.

Toda conectividad remota debe ser autenticada usando autenticación fuerte o con más de una contraseña (tales como el uso de contraseñas en conjunto con otras claves).

Todo dato transferido en una conexión remota debe ser encriptado, para protegerlo de que sea revelado a usuarios no autorizados.

Todas las políticas de seguridad que se aplican en el ambiente normal de trabajo en la oficina también deben aplicarse cuando se utilizan los recursos desde un ambiente externo.

Cualquier equipo personal, tales como computadoras que se utilicen para conectarse al sistema del Senado, deben cumplir con los requisitos para acceso remoto tales como tener programas antivirus y firewalls instalados y actualizados.

No se deberá almacenar datos en ninguna computadora que no pertenezca al sistema del Senado.

Es responsabilidad de los empleados asegurarse que los dispositivos que se están utilizando para el acceso remoto no sean usados por personas no autorizadas (tales como otros miembros de la familia).

Descripción del Procedimiento

- A) La OTI utiliza para conexión remota el servicio LogMeIn, que se puede acceder a través de Internet.
- B) La OTI determina los servidores donde se debe instalar la conexión a este servicio, así como los usuarios que podrán conectarse remotamente. Al autorizar a un usuario a conectarse remotamente, se le alertará sobre su obligación de cumplir con las políticas de seguridad establecidas por el Senado y las responsabilidades que conlleva.
- C) El Director o encargado de la oficina será responsable de la cuenta de LogMeIn que permite el acceso remoto a los servidores de la red y a su vez brindarla a los usuarios designados de la OTI. Para acceder a éstos, el usuario deberá ingresar el mismo “User-Id” y “password” que utiliza dentro de la red del Senado.
- D) El encargado de la seguridad deberá mantener una bitácora de los usuarios que acceden al sistema de esta manera.
- E) El encargado de la seguridad revisará por lo menos una vez al mes las estadísticas del sistema *LogMeIn*, para monitorear el uso del mismo.
- F) En caso de separación de empleo de algún usuario del sistema, el Director de la OTI deberá cambiar la contraseña del sistema de LogMeIn.

Responsabilidad

- A) Los propietarios de la información son responsables de asegurarse que el acceso remoto a la información se hace de acuerdo con los procedimientos aquí establecidos.
- B) Los usuarios de la información son responsables de:
 - 1. Cumplir con las guías y procedimientos que se establecen en esta política.
 - 2. Proteger la divulgación de las credenciales para el acceso remoto y los dispositivos de usuarios no autorizados.
 - 3. Reportar cualquier sospecha de acceso remoto no autorizado.
 - 4. La OTI es responsable de auditar el uso remoto para asegurar que se está cumpliendo con los procedimientos y guías que se han fijado en esta política.

Glosario

Autenticación: Proceso de verificar que un usuario es el que pretende ser. Estas técnicas se dividen en dos categorías: 1) algo que el usuario sabe, tal como la contraseña o el PIN, 2) algo que el usuario tiene, como un número de tarjeta, y 3) algo que es parte del usuario, y que cae en el campo de la biometría, tal como las huellas digitales o la lectura del iris.

Encriptar: Es el proceso mediante el que un texto se convierte en algo que es ilegible (utilizando un código), para propósitos de seguridad o privacidad. Los datos son codificados para prevenir acceso no autorizado.

Acceso remoto: Cualquier acceso a la red del sistema del Senado, a través de un dispositivo o medio que no es controlado por la oficina, tal como el acceso utilizando la red Internet, las líneas telefónicas, una conexión inalámbrica u otra conectividad externa.

Datos sensitivos: Cualquier dato que esté categorizado como “sensitivo” según los criterios de la Oficina de Tecnología e Informática.

PROCEDIMIENTO PARA ATENDER CAÍDAS DEL SISTEMA

Propósito

Planificar las actividades que se deben llevar a cabo en caso de caídas del sistema.

Alcance

Este procedimiento se dirige a identificar las causas de la caída del sistema y su clasificación como Falla Menor o Falla Mayor, así como el procedimiento que se deberá seguir para atender fallas menores. Para fallas mayores, los procedimientos a seguir están contemplados en el Plan de Contingencia.

Política

La OTI atenderá con la máxima prioridad aquellas situaciones de caídas en el sistema y evaluará la misma, de acuerdo con lo establecido en el Plan de Contingencia.

Descripción del Procedimiento

Evaluación de la Caída

Tan pronto como ocurra una falla del sistema, se deberá hacer una evaluación tan rápida como sea posible para tasar la naturaleza y extensión de la falla. El propósito de esta evaluación es obtener información relevante y determinar las mejores estrategias para recuperar el sistema. Se deberán efectuar las siguientes actividades:

- A) Verificar la causa de la interrupción del sistema, incluyendo tipo, alcance, localización y tiempo estimado de la interrupción.

- B) Verificar si la interrupción está localizada en un área o si es total.
- C) Verificar cuáles son los componentes que están fallando y los usuarios que están sin servicio.
- D) Verificar el impacto de la interrupción de los componentes que están dañados.
- E) Verificar el estatus funcional de todos los componentes del sistema (ej., completamente funcionales o parcialmente funcionales)
- F) Verificar la posibilidad de interrupciones adicionales o de daños al sistema.
- G) Verificar componentes que necesiten ser reemplazados (ej., hardware, software, firmware).
- H) Verificar tiempo que se anticipa que el sistema estará abajo (ej., no más de dos días).
- I) Clasificar la interrupción como “Falla menor del sistema o Falla Mayor del sistema”.
- J) Si la falla se clasifica como una Falla Menor del Sistema, se procederá a informar al Coordinador del Plan de Contingencia sobre el estimado de tiempo de recuperación. El Coordinador notificará a todos los usuarios del sistema que la “Falla Menor” está siendo atendida y estará en condiciones normales dentro del período de tiempo estimado.
- K) Si la falla se clasifica como una Falla Mayor del Sistema, se activará el Plan de Contingencia y se procederá según se ha establecido en el documento escrito para tal fin.

Si la falla se presenta en el sistema de comunicaciones, se deberán llevar a cabo las siguientes actividades:

- A) Se procederá a verificar el equipo de comunicaciones: switches y líneas T1.
- B) A las líneas T1, se procederá a darles Reset. Si el problema persiste, se procede a llamar al proveedor del servicio.
- C) Si el problema es con los switches, se les dará Reset y se analizará si alguna línea está dando colisión, o si hay ruptura en un cable.
- D) Si el problema persiste, identificándose que se trata de un problema mecánico del switch, se llamará al suplidor para propósito de garantía y reemplazo.

PROCEDIMIENTOS PARA LA EVALUACIÓN, ADQUISICIÓN, DESARROLLO, MODIFICACIÓN E IMPLEMENTACIÓN DE PROGRAMAS Y APLICACIONES

Propósito

Presentar las normas y procedimientos a seguir para la evaluación, adquisición, desarrollo, modificación, e implementación de programas y aplicaciones en los sistemas de información del Senado de Puerto Rico.

Alcance

El alcance de este procedimiento aplicado a todos los empleados y contratistas que laboren en la Oficina de Tecnología e Informática (OTI) del Senado de Puerto Rico.

Política

Este documento pretende establecer las normas y procedimientos para las siguientes fases de un proyecto informático: 1) Evaluación, Análisis y Planificación, 2) Desarrollo y Pruebas, 3) Implementación, 4) Operacional, 5) Conservación y Control de Cambio.

Cada una de estas fases conlleva la implementación de controles y de métodos de seguridad. Además, en cada etapa se recomienda establecer un proceso de revisión de calidad de los productos.

Proceso de Pre Implantación

Como parte de este proceso, se identifican y se definen todas las tareas o actividades previas a la instalación del sistema.

El estudio de la necesidad nos ayudará en la creación del plan de desarrollo de tecnología y a establecer las prioridades entre unas necesidades y otras: áreas críticas y menos críticas. En este Plan se indica el sistema, prioridad del proyecto, programas necesarios, equipo y sus requisitos mínimos. También es necesario indicar las fases, sus tareas, recurso asignado (segregación de tareas) y fecha de terminación. Los programas para el desarrollo de sistemas y de programas deben de contener como mínimo los siguientes puntos:

- Descripción específica de los productos que se van a entregar.
- Fecha para la entrega de los productos.
- Compromiso de documentación, mantenimiento, actualización.
- Adiestramiento.
- Descripción del apoyo que se brindará durante la instalación
- Criterios para la aceptación por el usuario
- Disposición para permitir un periodo razonable de prueba

- Aceptación

Proceso de Implementación

La implementación de un nuevo sistema es un proceso complejo que requiere la interacción de los usuarios, el equipo de desarrollo, y el grupo de procesamiento de la Oficina de Tecnología e Informática. Este proceso comprende la instalación, la conversión de archivos, el adiestramiento de los usuarios y de los operadores del nuevo sistema, y la revisión y la actualización de la documentación. La prueba de aceptación se lleva a cabo en esta etapa. Los pasos que se deben seguir para la implementación son los siguientes:

- Establecer y llevar a cabo el plan de implementación.
- Establecer y llevar a cabo el plan de conversión, si aplica.
- Preparar respaldo y estrategia de recuperación para el nuevo sistema.
- Establecer una función de monitoreo.
- Preparar la documentación del sistema (manual del sistema, manual de usuario, manual de operación de computadoras, “*help desk*” y de control de redes entre otros).
- Adiestrar a los usuarios en la operación del sistema nuevo o revisado.
- Establecer la operación del sistema paralelo de ser necesario durante proceso de conversión.
- Realizar una revisión de los procedimientos para asegurar que existan los siguientes controles y/o establecer las tareas a ser realizadas para cumplir con ellos:
 - Seguridad Física
 - Seguridad Lógica
 - Resguardo
 - Plan de Contingencia (Continuidad de las Operaciones y Recuperación de Desastre)
 - Uso de los equipos incluyendo el Internet y Correo Electrónico
 - Control de cambio de los equipos y programas
 - Disposición de los equipos
 - Uso y control de las licencias de programas

Proceso de Post-Implementación

La evaluación post-implementación es la última fase del ciclo de desarrollo de sistemas consiste en una revisión que se realiza después que el sistema de información haya sido instalado. Dicha evaluación debe realizarla un grupo compuesto por el personal encargado, los usuarios del sistema y los programadores. Estos deben de evaluar si se logró satisfacer los objetivos establecidos.

Proceso de Control de Cambios

Una vez los sistemas han sido implementados y estén corriendo, pueden surgir pedidos por parte de los usuarios que lo utilizan. Para llevar a cabo cualquier tipo de modificación, es necesario

llevar un registro de pedidos y las acciones que se llevarán a cabo para efectuarlos. Estos cambios se deben hacer en un ambiente de prueba y no de producción. Luego serán sometidos al usuario para que evalúe si se logró satisfacer los objetivos establecidos. Una vez aprobados, serán sometidos a producción por la persona asignada por el Director de la OTI.

Procedimiento

Pre Implementación

Al surgir la necesidad de una nueva aplicación y/o equipo tecnológico el usuario en conjunto con la Oficina de Tecnología e Informática debe seguir los siguientes pasos:

- El usuario informará al Director de la Oficina de Tecnología e Informática la necesidad. La forma completada será entregada al Director de la Oficina de Tecnología e Informática para evaluación y aprobación. El Director de la Oficina de Tecnología e Informática se reunirá con la Administración del Senado para evaluar el proyecto. Si la data a ser manejada no es crítica, de carácter sensitivo o valor considerable entonces no se requiere especificaciones escritas. En este caso no se requerirá el desarrollo de un Plan de Desarrollo Tecnológico.
- Una vez aprobado el proyecto, el usuario en conjunto con la Oficina de Tecnología e Informática desarrollará el un plan de desarrollo. El contenido de este documento está descrito a continuación:
 - Introducción: Descripción específica de los productos que se van a entregar y su relación con la necesidad del usuario.
 - Especificaciones: Descripción detallada de las especificaciones del sistema.
 - Plan de Trabajo: Plan de tareas incluyendo análisis, diseño. Documentación, pruebas, conversión, implementación, aceptación y adiestramiento. El plan debe de incluir fecha y recursos asignados.
 - Descripción de Roles: Descripción de roles y la asignación de recursos a cada rol
 - Aprobación: Este documento debe de ser aprobado por el usuario, la Oficina de Tecnología e Informática y el Personal encargado.

Implementación

La fase de implementación consiste en la evaluación de los objetivos establecidos en el Plan de Desarrollo Tecnológico para asegurar que estos fueron completados. Con este propósito se seguirá los siguientes pasos:

- El usuario en conjunto con el personal encargado completarán el formulario designado.

- Luego de ser completado, este será entregado al Director de la OTI para revisión y aprobación.
- Una vez aprobado la fase de implementación se procede a evaluar el cierre del proyecto bajo la fase de Post-Implementación

Post-Implementación

La última fase del ciclo de desarrollo consiste en la evaluación de los objetivos para asegurar que estos fueran completados. Con este propósito se seguirán los siguientes pasos:

- El usuario en conjunto con la persona encargada desarrollarán y ejecutarán las pruebas. Se describirá todas las pruebas a ser realizadas y el resultado esperado. La ejecución de este proceso debe proveer al usuario las pruebas necesarias para la aprobación y cierre del proyecto.
- Una vez culminado el proyecto la documentación será archivada.
- Notificar a los usuarios de que el sistema está listo para ser utilizado.

Control de Cambios

El control de cambios es la pieza clave para el monitoreo de pedidos y modificaciones a un sistema. Para llevar éstos a cabo se deberán seguir los siguientes pasos:

- El usuario notificará la modificación deseada al Director de la OTI o su encargado, con el nombre de la aplicación y los cambios que se necesitan.
- El equipo de programación analizará la petición y contestará en un tiempo razonable al peticionario si los cambios son viables o no y la fecha aproximada de culminación.
- El programador hará los cambios necesarios en un ambiente de prueba.
- El programador efectuará las pruebas necesarias.
- Una vez aprobados los cambios serán puestos en producción por el encargado del proceso de control de cambios.