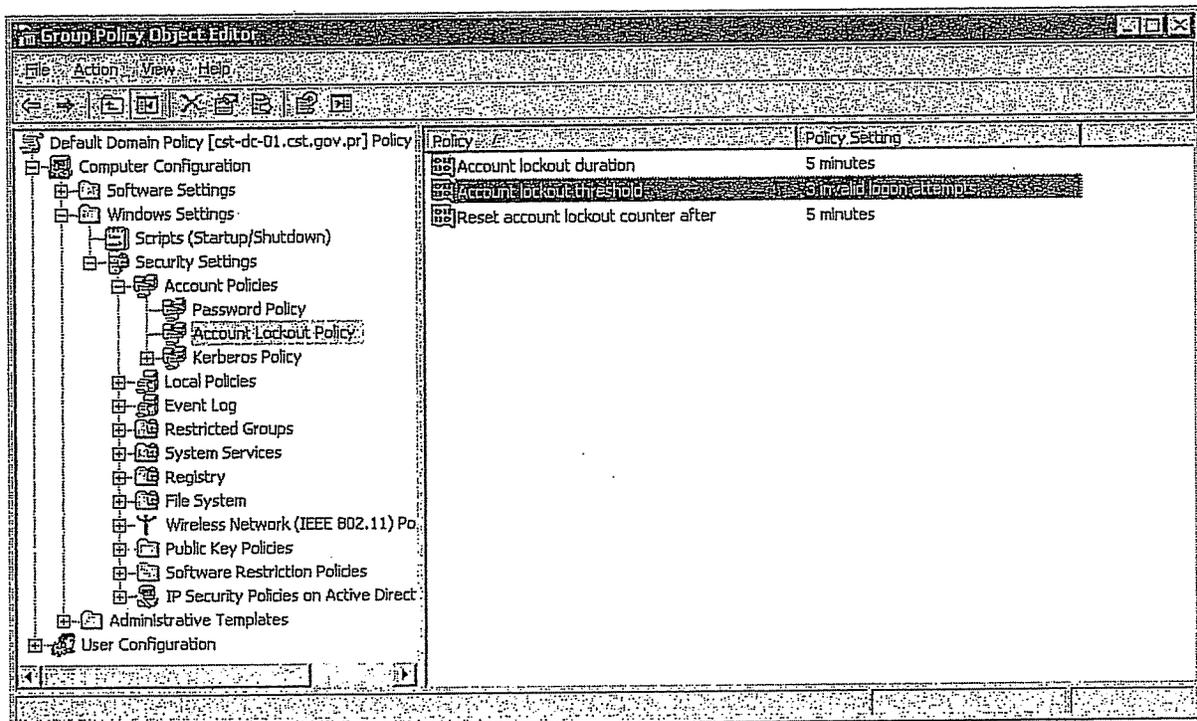


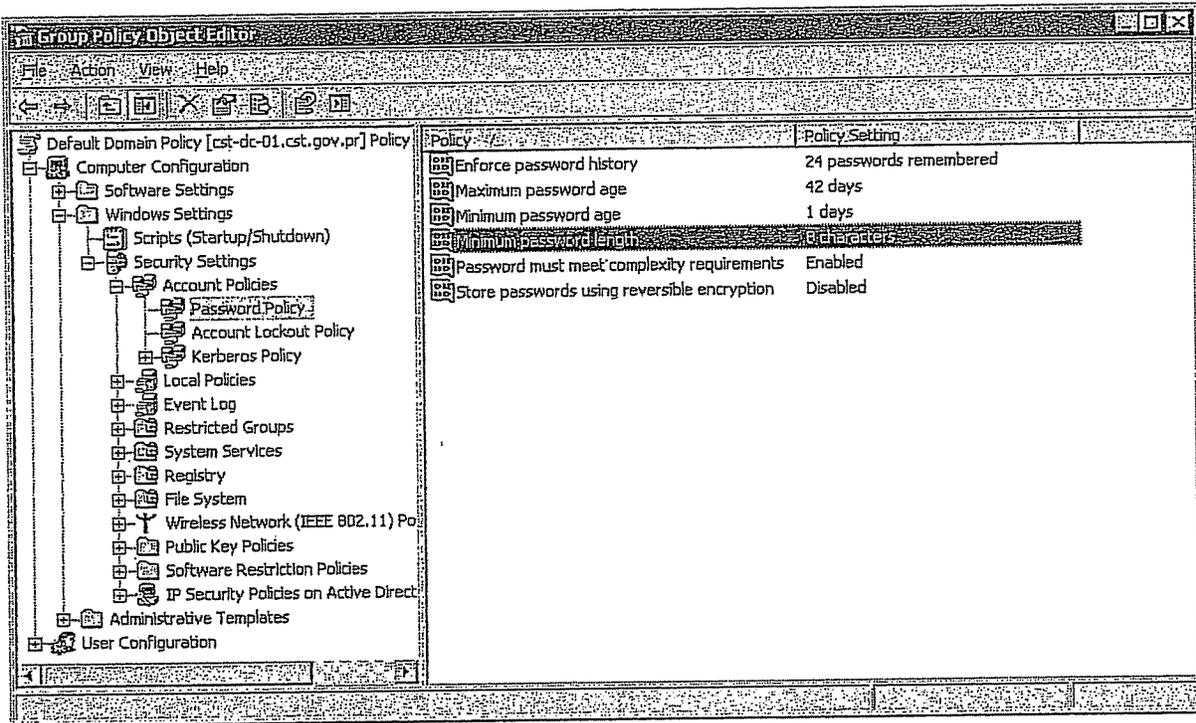
Anejo A

Por este medio certificamos que la CST ha iniciado los procesos necesarios para implantar las recomendaciones requeridas para atender los siguientes hallazgos:

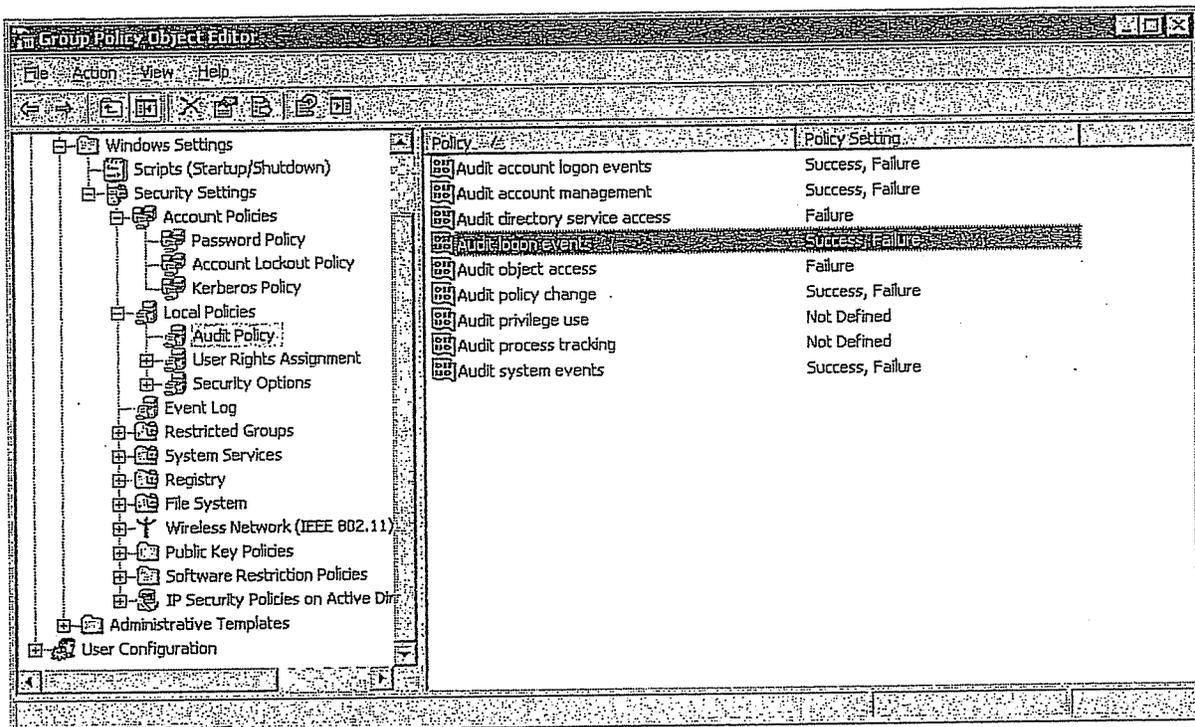
- Actualmente se esta trabajando con el análisis de las paginas electrónicas requeridas por el personal según sus funciones para ser revisada por la Directora Auxiliar de Operaciones y luego ser implementadas en el ISA Server.
- Actualmente se esta trabajando con el análisis de los correos electrónicos externos requeridos por el personal según sus funciones para ser revisado por la Directora Auxiliar de Operaciones y luego ser implementadas en el ISA Server y el Exchange Server según requerido.
- Se restringió el horario y días de acceso de cada usuario según las funciones de cada empleado.
- Se configuró la opción de desconectar automáticamente las cuentas de acceso de aquellos usuarios que realicen tres intentos sin éxito para acceder los recursos de la red:



- Se estableció un mínimo de ocho caracteres para la utilización de las contraseñas:



- Se activaron las opciones correspondientes en la pantalla de políticas de auditoría (Audit Policies) de manera que se pueda mantener un rastro de las actividades realizadas en los servidores de la Comisión:



Software Development International

- Las llaves de las puertas de los servidores actualmente están localizadas en lugar seguro. Las puertas delanteras de los gabinetes de servidores actualmente están cerradas. Actualmente se está trabajando con la reubicación de la cabrería que entra a los gabinetes de los servidores para poder cerrar correctamente las puertas de atrás.
- Actualmente se está trabajando con la elaboración de un plan de acción referente a la reubicación, identificación y protección del cableado que entra a los gabinetes de los servidores.

De surgir alguna duda relacionada a estos asuntos, por favor no dude en comunicarse con nosotros a su mejor conveniencia.



Kenny Monell

Administrador de Redes

Software Development International

kmonell@sdipr.net

Anejo B

"NORMAS SOBRE EVALUACIÓN DE RIESGOS"

Asumo: Área de Auditoría Interna, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-03

Página 1 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

I INTRODUCCIÓN

La Oficina del Contralor de Puerto Rico, mediante Carta Circular OC-06-32, propone el establecimiento voluntario del Programa de Prevención-Anticorrupción como alternativa para mantener una administración pública de excelencia y promover el uso efectivo y eficiente de los recursos del gobierno en beneficio de la sociedad puertorriqueña. La Comisión para la Seguridad en el Tránsito, comprometida en colaborar con este esfuerzo, a partir del 2006 decidió establecer el Programa.

En la Carta Circular OC-06-31, la Oficina del Contralor de Puerto Rico incluye el desglose de los criterios que serán evaluados por ellos en futuras Evaluaciones de Criterio que realicen. Entre los nuevos criterios, incluyen uno exclusivamente dedicado a la evaluación de este Programa.

La evaluación de riesgos además de que promueve la eficiencia operacional a todos los niveles:

- es parte esencial de la gestión estratégica de toda entidad
- se centra en la identificación y tratamiento de éstos, para añadir valor a las actividades de la entidad
- respalda la responsabilidad, la medida y la recompensa del rendimiento

II BASE LEGAL

Esta norma tiene como base legal y reglamentaria una serie de disposiciones contenidas en los siguientes documentos:

- Ley Núm. 33 del 25 de mayo de 1972, crea la Comisión para la Seguridad en el Tránsito, según enmendada
- Ley Núm. 12 de 24 de julio de 1985 - Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico, según enmendada
- Ley Núm. 84 del 18 de junio de 2002 - Ley para Establecer un Código de Ética para Contratistas, Proveedores de Bienes y Servicios y Solicitantes de Incentivos Económicos
- Ley Núm. 426 de 7 de noviembre de 2000 - Ley para la Protección de los Derechos de los Empleados y Funcionarios Públicos Denunciantes, Querellantes o Testigos de Alegados Actos Constitutivos de Corrupción
- Reglamento Núm. 4827 de 20 de noviembre de 1992 - Reglamento de Ética Gubernamental, según enmendado

"NORMAS SOBRE EVALUACIÓN DE RIESGOS"

Asunto: Área de Auditoría Interna, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-08

Página 2 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

III. PROPÓSITO

Establecer las normas con el propósito de la identificación y análisis de los riesgos que afectarían el logro de los objetivos, para determinar cómo deben ser atendidos.

IV. APLICABILIDAD

Estas normas aplicarán a todo el personal de la CST.

V. DETERMINACIÓN

Al realizar una evaluación de riesgo se debe tomar en consideración lo siguiente:

- Identificación del riesgo
- Estimación del riesgo
- Determinación de los objetivos de control
- Detección del cambio

2. Identificación del riesgo

Se deben identificar los riesgos relevantes que enfrenta un organismo en la persecución de sus objetivos, ya sean de origen interno como externo. Esto mediante un Plan Estratégico que incluya áreas: operacionales, de reportes, cumplimiento.

La identificación del riesgo es un proceso iterativo, y generalmente integrado a la estrategia y planificación. En este proceso es conveniente "partir de cero", esto es, no basarse en el esquema de riesgos identificados en estudios anteriores. En adición, se debe identificar los riesgos para determinar eventos que afectaron el logro de los objetivos (operacionales, financieros, cumplimiento) – en relación a los componentes del control interno. Esto como:

- Tipo (Negativo, positivo)
- Origen (Interno, externo)
- Relación al objetivo (Inherente, Residual)
- Perspectiva (Ocurrencia y/o probabilidad, impacto y/o efecto)

Su desarrollo debe comprender la realización de un "mapeo" del riesgo, que incluya la especificación de los dominios o puntos claves del organismo, la identificación de los objetivos generales y particulares, y las amenazas y riesgos que se pueden tener que afrontar.

Un dominio o punto clave del organismo, puede ser:

- un proceso que es crítico para su sobre vivencia;
- una o varias actividades que sean responsables de la entrega de porciones importantes de servicios a la ciudadanía;
- un área que está sujeta a Leyes, Decretos o Reglamentos de estricto

"NORMAS SOBRE EVALUACIÓN DE RIESGOS"

Asunto: Área de Auditoría Interna, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-08

Página 3 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

- cumplimiento, con amenazas de severas puniciones por incumplimiento; un área de vital importancia estratégica para el Gobierno (ejemplo: defensa, investigaciones tecnológicas de avanzada).

Al determinar estas actividades o procesos claves, fuertemente ligados a los objetivos del organismo, debe tenerse en cuenta que pueden existir algunos de éstos que no están formalmente expresados, lo cual no debe ser impedimento para su consideración. El análisis se relaciona con la criticidad del proceso o actividad y con la importancia del objetivo, más allá que éste sea explícito o implícito.

Existen muchas fuentes de riesgos, tanto internas como externas. A título puramente ilustrativo se pueden mencionar, entre las externas:

- desarrollos tecnológicos que en caso de no adoptarse, provocarían obsolescencia organizacional;
- cambios en las necesidades y expectativas del ciudadano/usuario;
- modificaciones en la legislación y normas regulatorias que conduzcan a cambios forzados en la estrategia y procedimientos;
- alteraciones en el escenario económico que impacten en el presupuesto del organismo, sus fuentes de financiamiento y su posibilidad de expansión.

Entre las internas, podemos citar:

- la estructura organizacional adoptada, dado la existencia de riesgos inherentes típicos tanto en un modelo centralizado como en uno descentralizado;
- la calidad del personal incorporado, así como los métodos para su instrucción y motivación;
- la propia naturaleza de las actividades del organismo.

Una vez identificados los riesgos a nivel del organismo, deberá practicarse similar proceso al nivel de programa y actividad. Se considerará, en consecuencia, un campo más limitado, enfocado a los componentes de las áreas y objetivos claves identificadas en el análisis global del organismo. Los pasos siguientes al diagnóstico realizado son los de la estimación del riesgo y la determinación de los objetivos de control.

b. Estimación del riesgo

Se debe estimar la frecuencia con que se presentarán los riesgos identificados, así como también se debe cuantificar la probable pérdida que ellos pueden ocasionar.

Una vez identificados los riesgos al nivel de organismo y de programa/actividad, debe procederse a su análisis. Los métodos utilizados para determinar la importancia relativa de los riesgos pueden ser diversos, e incluirán como mínimo:

- una estimación de su frecuencia, o sea la probabilidad de ocurrencia.
- una valoración de la pérdida que podría resultar.

"NORMAS SOBRE EVALUACIÓN DE RIESGOS"

Asunto: Área de Auditoría Interna, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-08

Página 4 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

En general, aquellos riesgos cuya concreción esté estimada como de baja frecuencia, no justifican preocupaciones mayores. Por el contrario, los que se estima de alta frecuencia deben merecer preferente atención. Entre estos extremos se encuentran casos que deben ser analizados cuidadosamente, aplicando elevadas dosis de buen juicio y sentido común.

Existen muchos riesgos dificultosos de cuantificar, que como máximo se prestan a calificaciones de "grande", "moderado" o "pequeño". Pero no debe cederse a la difundida inclinación de conceptuarlos rápidamente como "no medibles". En muchos casos, con un esfuerzo razonable, puede conseguirse una medición satisfactoria.

Esto se puede expresar matemáticamente en la llamada Ecuación de la Exposición:

$$PE = F \times V$$

en donde:

PE = Pérdida Esperada o Exposición, expresada en pesos y en forma anual.
 F = Frecuencia, veces probables en que el riesgo se concrete en el año.
 V = Pérdida estimada para cada caso en que el riesgo se concrete, expresada en pesos.

Por ser esta una tarea que requiere mas esfuerzo y conocimiento técnico la CST optó por evaluar los riesgos mediante el método cualitativo = opinión (visión) sobre la ocurrencia (impacto) del evento. Para esto utiliza la siguiente tabla:

Estado Libre Asociado de Puerto Rico					
Comisión para la Seguridad en el Tránsito					
EVALUACIÓN DE RIESGOS					
Año XXXX					
EVALUACIÓN DE RIESGO					
(1) OBJETIVO	(2) O, F, C	(3) FACTOR (EVENTO)	(4) OCURRENCIA	(5) ACTIVIDAD CONTROL	(6) CONCLUSIÓN

- (1) Describir EL objetivo que se persigue. Ej.: Que las órdenes de compra se completen a tiempo.
- (2) Clasificar el Objetivo: O = operacional; F = De reporte (Financiero); C = Cumplimiento.
- (3) Describir el evento - ¿Qué ocurría que evitaría el logro del objetivo? Ej. El formulario se pierde y se retrasa su procesamiento.
- (4) Opinión (clasificar probabilidad); Mucho (alto) = 5; Poco (Mediano) = 3; Ninguna (Bajo) = 0.

"NORMAS SOBRE EVALUACIÓN DE RIESGOS"

Asunto: Área de Auditoría Interna, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-08

Página 5 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

- (5) Identifica aquellas relacionadas al objetivo y al riesgo. Ej. Informe semanal de OC pendientes.
- (6) Las actividades. ¿Suficientes, adecuadas? Para evitar o manejar el riesgo. Recomendaciones (acción).

c. Determinación de los objetivos de control

Luego de identificar los riesgos, el Director Ejecutivo de la CST debe determinar los objetivos específicos de control y, con relación a ellos, establecer los procedimientos de control más convenientes, o sea, establecer un plan de acción.

Una vez que la Dirección Superior y las Gerencias han identificado y estimado el nivel de riesgo, deben adoptarse las medidas para enfrentarlo de la manera más eficaz y económica posible.

Se deberán establecer los objetivos específicos de control del organismo, que estarán adecuadamente articulados con sus propios objetivos globales y sectoriales.

En función de los objetivos de control determinados, se seleccionarán las medidas o salvaguardas que se estimen más efectivas al menor costo, para minimizar la exposición.

d. Detección del cambio

Todo organismo debe disponer de procedimientos capaces de captar e informar oportunamente los cambios registrados o inminentes en el ambiente interno y externo, que puedan conspirar contra la posibilidad de alcanzar sus objetivos en las condiciones deseadas.

Una etapa fundamental del proceso de Evaluación del Riesgo es la identificación de los cambios en las condiciones del medio ambiente en que el organismo desarrolla su acción. Un sistema de control puede dejar de ser efectivo al cambiar las condiciones en las cuales opera.

A este proceso de identificar cambios efectivos o potenciales con vistas a adoptar las decisiones oportunas, se lo denomina gestión de cambio. Requiere un sistema de información apto para captar, procesar y transmitir información relativa a los hechos, eventos, actividades y condiciones que originan cambios ante los cuales el organismo debe reaccionar.

Involucra la identificación de los cambios y el análisis de las oportunidades y riesgos asociados. Esto es, identificar causas potenciales que faciliten o impidan alcanzar los objetivos, calcular la probabilidad de su ocurrencia, evaluar sus probables efectos, y considerar el grado en que el riesgo puede ser controlado o la oportunidad aprovechada.

"NORMAS SOBRE EVALUACIÓN DE RIESGOS"

Asunto: Área de Auditoría Interna, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-08

Página 6 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogada: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

A título de ejemplo se señalan algunas condiciones que deben merecer particular atención

- Cambios en el contexto externo: legislación, reglamentos, programas de ajuste, tecnología, cambios de autoridades, etc.
- Crecimiento acelerado: un organismo que crece a un ritmo demasiado rápido está sujeto a muchas tensiones internas y a presiones externas.
- Reorganizaciones: generalmente significan reducciones de personal que ocasionan, si no son racionalmente practicadas, alteraciones en la separación de funciones y en el nivel de supervisión.
- Creación del sistema de información o su reorganización: puede llegar a generar un período de exceso o defecto en la información producida, ocasionando en ambos casos la probabilidad de decisiones incorrectas.

El proceso de gestión de cambio es crítico para el Sistema de Control Interno y no debe ser obviado en ninguna circunstancia.

VI INSTRUCCIONES A SER OBSERVADAS

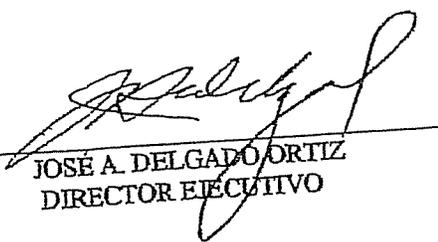
Será responsabilidad de cada Director de Área, informar a todo el personal de las "Normas sobre Evaluación de Riesgos, CST-N-08". De igual manera, cada supervisor deberá proveer copia de esta Norma a todo empleado bajo su supervisión.

VII DEROGACIÓN

No aplica.

VIII VIGENCIA

Las disposiciones promulgadas en esta Norma comenzarán a regir inmediatamente después de su aprobación y derogan cualquier norma o disposición en conflicto con las mismas.



JOSÉ A. DELGADO ORTIZ
DIRECTOR EJECUTIVO

28 de diciembre de 2007
FECHA

Anejo C

"NORMAS SOBRE EL USO DE SISTEMAS ELECTRÓNICOS"

Asunto: Área de Informática, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-01

Página 1 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

I. PROPÓSITO

La Comisión para la Seguridad en el Tránsito (CST), con el propósito de lograr acceso a computadoras, redes, servicios electrónicos internos y a la red Internet, resulta necesario adoptar normas y condiciones que viabilicen dichos objetivos.

Como complemento de dichas normas, se ha implantado el documento para la divulgación y aceptación de la "Política Sobre el Uso de Internet y Correo Electrónico", codificado bajo el número CST-POL-02, cuya aceptación y firma, por parte del usuario, constituirá un requisito indispensable para la concesión de privilegios de usuario en el sistema. Dicho documento se implantará como parte de la política aquí promulgada y se incluirá en la creación de cada cuenta nueva.

Así mismo, los expedientes de cada usuario en el sistema serán actualizados y se le adjuntará, una copia de la "Política CST-POL-02", debidamente recibida y aceptada por dicho usuario.

II. APLICABILIDAD

Las disposiciones contenidas en esta Norma serán de aplicación a todo funcionario o empleado de la CST. El (la) Oficial Principal de Informática será responsable de emitir y que se apruebe toda norma o política necesaria para el buen funcionamiento del sistema y estas serán de aplicabilidad general.

III. DISPOSICIONES GENERALES

Será requisito para utilizar una computadora dentro del sistema y acceder los servicios asociados, el entender y aceptar las siguientes normas y condiciones:

A. Titularidad y Derechos

1. Toda computadora, equipo, los servicios asociados, tanto internos como externos, el sistema de correspondencia electrónica ("e-mail"), la Intranet, el acceso a la Internet y los documentos y programas que existen en la misma, son propiedad de la CST y solo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de esta.
2. Toda información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de una de las computadoras de la CST, será propiedad de esta, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.

"NORMAS SOBRE EL USO DE SISTEMAS ELECTRÓNICOS"

Asunto: Área de Informática, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-01

Página 2 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

3. La información contenida en cualquier computadora, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica ("e-mail"), información de la Intranet o la Internet y los documentos y programas existentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes de la CST.
4. Se prohíbe terminantemente utilizar programas o recursos para los cuales no exista una licencia o autorización de uso válido a nombre de la CST.
5. Se prohíbe terminantemente copiar programas de la CST para instalarlos en otras computadoras, sin la autorización por escrito de la (el) Oficial Principal de Informática.
6. Se prohíbe terminantemente el instalar programas en las computadoras de la Agencia sin la autorización por escrito de la (el) Oficial Principal de Informática.
7. Se prohíbe el uso de los sistema de computadoras y comunicaciones de la CST para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y envío de mensajes de cadena. De igual forma, el usuario no podrá utilizar los recursos electrónicos de la CST para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a las funciones de la CST.
8. Se prohíbe acceder a, o utilizar propiedad intelectual ("copyrighted information") que viole los derechos del autor.

B. Seguridad

1. El uso de un código de acceso ("password"), tiene como objetivo la protección y confidencialidad de la información oficial contenida en el sistema, el mismo no significa que el usuario alberga expectativa de intimidad alguna con relación a la información almacenada en la computadora, así mismo, tampoco impedirá que el sistema sea auditado por los administradores de este. Las contraseñas deben mantenerse en estricta confidencialidad y administrarse conforme a las medidas de seguridad adoptadas por la CST. Al aceptar y utilizar el sistema de computadoras el empleado reconoce haber leído y entendido las medidas de seguridad de contraseñas establecidas.
2. La CST se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computarizados para garantizar que su propiedad se utilice para los propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente o al azar, o cuando exista una investigación sobre una situación en particular. Por estas circunstancias, el personal de la CST no tiene derecho a la intimidad con relación a cualquier información, documento o mensaje creado, recibido o enviado a través del sistema de e-mail.

"NORMAS SOBRE EL USO DE SISTEMAS ELECTRÓNICOS"

Asunto: Área de Informática, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-01

Página 3 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

3. Para evitar poner en peligro la confidencialidad de la información de la CST, se prohíbe el envío fuera de estas, de documentos electrónicos o mensajes por medio del e-mail que contenga información confidencial.
4. Se prohíbe el envío o recibo de mensajes de correo electrónico o de cualquier tipo entre el personal de la CST con otras personas que no pertenezcan a la CST, en los cuales se divulgen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a situaciones, controversias, problemas, malentendidos, funcionamiento, políticas, personas o cualquier otra situación o asunto interno de la CST, que puedan poner en entredicho la reputación o imagen de la misma, aunque la información divulgada no sea de naturaleza confidencial.
5. Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.
6. Se prohíbe codificar, asignar contraseñas o modificar de alguna manera la información, mensajes de correo electrónico o archivos propiedad de la CST con el propósito de impedir que alguien pueda leerlos, entenderlos o utilizarlos, o con el propósito de falsear o alterar el nombre del usuario, la fecha de creación o modificación u otra información que se utilice regularmente para identificar la información, mensajes o archivo, si no se obtiene previamente el consentimiento por escrito del Director Ejecutivo de la CST o por el (la) Oficial Principal de Informática. En el caso de que por razones de seguridad se permita codificar, asignar contraseñas o modificar alguna información electrónica a fines de evitar que otras personas puedan leerla, la CST estarán facultados para decodificar la misma o restituirla a su condición original, y el usuario será responsable de proveer todos los datos para lograr acceso a la información o archivo electrónico.
7. Se prohíbe la modificación de los parámetros o configuración de las computadoras de la CST para darle la capacidad de recibir llamadas telefónicas o cualquier otro tipo de acceso o conexión remota que permita instrucciones no autorizadas a la red de la CST.
8. Se prohíbe el uso de discos magnéticos o cualquier otro medio de almacenaje de información, sin que haya sido verificado o certificado como libre de virus. Para ello se debe seguir el procedimiento de seguridad previamente establecido.
9. Todos los archivos que se creen en las computadoras deben guardarse en el directorio asignado a cada usuario con el propósito de que puedan protegerse mediante los mecanismos de resguardo ("backup") existentes.

"NORMAS SOBRE EL USO DE SISTEMAS ELECTRÓNICOS"

Asunto: Área de Informática, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-01

Página 4 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

C. Políticas Anti-discrimen

1. Estará prohibido absolutamente y no será tolerada la utilización de la computadora o del sistema de correspondencia electrónica para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razón de raza, género, credo, ideas políticas u origen social o nacional, o que puedan ser catalogados como de hostigamiento sexual.
2. Está prohibido el manejo o transmisión de material obsceno, profano u ofensivo a través del sistema de computadoras o del sistema de comunicación electrónica de la CST. Eso incluye, a modo de ejemplo, acceso a materiales eróticos, bromas de cualquier forma o cualquier comentario o chiste que pueda violar la política de discrimen de la Agencia o su política de hostigamiento sexual.
3. Se prohíbe que se utilicen protectores de pantalla de monitor ("screen savers") con fotos de personas, artistas, modelos, deportistas, fotos de calendario o cualquier otra imagen que pueda resultar poco seria u ofensiva.
4. Se prohíbe la divulgación por cualquier medio de cualquier tipo de opiniones personales específicas con relación a raza, origen nacional, sexo, orientación sexual, edad, ideas o creencias religiosas o políticas, así como opiniones sobre personas con impedimento físico o mental.

D. Correo Electrónico

1. Se prohíbe que los usuarios utilicen durante horas laborables cuentas de correo electrónico distintas a las cuentas oficiales provistas por la Agencia.
2. Se prohíbe el envío a otras personas de copia de un mensaje de correspondencia electrónica recibido sin el consentimiento o consentimiento del remitente original.
3. Se prohíbe leer, revisar o interceptar cualquier tipo de comunicación electrónica de la CST o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de la comunicación.
4. Se prohíbe que los usuarios se suscriban a listas de correo electrónico o que participen en grupos de noticias ("new groups") que divulguen información o mensajes ajenos a las funciones y deberes de la CST.
5. No se podrán crear archivos o enviarlos mediante el correo electrónico que excedan la capacidad de la cuota del usuario en el servidor.

"NORMAS SOBRE EL USO DE SISTEMAS ELECTRÓNICOS"

Asunto: Área de Informática, Comisión para la Seguridad en el Tránsito

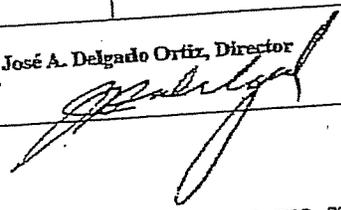
Norma Núm. CST-N-01

Página 5 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST



E. Otras Normas Aplicables

1. Se prohíbe el uso de programas de charlas ("Chats") a menos que sean autorizados expresamente por el Director Ejecutivo de la CST, o por el (la) Oficial Principal de Informática.
2. Las políticas antes mencionadas sobre el uso del correo electrónico y sus auditorías serán de igual aplicación para los otros recursos de la Intranet e Internet tales como: www, FTP, Chat y otros.
3. Es responsabilidad de los usuarios el cumplir con las normas de cuotas de espacio de los servidores.
4. Las políticas de Internet serán revisadas periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la CST.

F. Aceptación y procedimientos Disciplinarios

1. Se tomarán las medidas disciplinarias, civiles o criminales que correspondan contra los usuarios que violen estas políticas o abusen del acceso a la Internet, según sea el caso. En el caso de las medidas disciplinarias las mismas estarán acorde con la gravedad de la infracción y la severidad de las medidas disciplinarias establecidas en los Reglamentos o normas vigentes, o que puedan aprobarse. Estas medidas pueden ser desde una amonestación hasta la destitución, según establecido.
2. La CST se reserva el derecho de radicar acusaciones criminales por las actuaciones que constituyan delito federal o estatal aunque no estén expresamente prohibidas por estas condiciones de uso de los equipos de computadoras.
3. El hecho de que una conducta o actuación relacionada con las computadoras, redes, sistemas y recursos electrónicos de la CST no este contemplada en estas normas y condiciones de uso de las computadoras, no impide que el usuario pueda ser sancionado, si a juicio del encargado se trata de una conducta o actuación imprudente o irresponsable en relación a los referidos equipos y recursos electrónicos. A los fines de estas normas y condiciones de uso, una conducta o actuación imprudente o irresponsable significa cualquier acción directa o indirecta que ponga en riesgo la seguridad, integridad y confiabilidad de los equipos, las redes, la información, los programas y los sistemas de la CST. Uso imprudente o irresponsable significa además, cualquier actuación o conducta directa o indirecta que pueda ocasionar daño físico, mental, moral, problemas interpersonales o un menoscabo de la reputación de los usuarios o personas ajenas a la CST.
4. Será obligación de todo usuario, comunicar al el (la) Oficial Principal de Informática cualquier situación, incidente o problema de seguridad, acceso

"NORMAS SOBRE EL USO DE SISTEMAS ELECTRÓNICOS"

Asunto: Área de Informática, Comisión para la Seguridad en el Tránsito

Norma Núm. CST-N-01

Página 6 de 6

Fecha de efectividad
28 de diciembre de 2007

Norma derogado: N/A

Aprobado por: José A. Delgado Ortiz, Director Ejecutivo CST

indebido o violación voluntaria o involuntaria de estas normas, que surja en el uso de las computadoras o redes de la CST.

5. Se entenderá que todo empleado o funcionario que acepte la utilización del sistema electrónico, acepta como obligación el conocer y seguir todas las políticas o instrucciones de la CST en cuanto a las medidas de seguridad del uso del equipo de computadoras y de las redes disponibles, particularmente las normas adoptadas para la utilización del Internet.
6. Se entenderá que todo empleado o funcionario que acepte la utilización del sistema electrónico, ha recibido y entendido las normas divulgadas relacionadas con toda la información relacionada al uso de dicho sistema. Además, de haber duda en cuanto a alguna norma o condición se compromete a consultar la misma con el (la) Oficial Principal de Informática, autorizada (o) en esta Norma o en las "Política CST-POL-02".

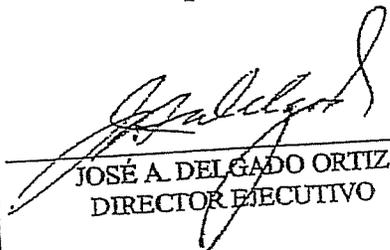
IV. INSTRUCCIONES A SER OBSERVADAS

Será responsabilidad de cada Director de Área, informar a todo el personal sobre la "Política CST-POL-02". De igual manera, cada supervisor deberá proveer copia de esta Norma y de dicha política a todo empleado bajo su supervisión.

V. DEROGACIÓN

VI. VIGENCIA

Las disposiciones promulgadas en esta Norma comenzarán a regir inmediatamente después de su aprobación y derogan cualquier norma o disposición en conflicto con las mismas.



JOSÉ A. DELGADO ORTIZ
DIRECTOR EJECUTIVO

28 de diciembre de 2007
FECHA

Anejo D



COMISIÓN PARA LA
SEGURIDAD EN EL TRÁNSITO
GOBIERNO DE PUERTO RICO

5 de octubre de 2011

TODO EL PERSONAL

Darnie Muñoz Marrero
Director Aux. de Administración

SOLICITUD DE SERVICIOS INFORMÁTICA

Con el propósito de mantener un control adecuado de las solicitudes de servicio de problemas de los sistemas de informática, solicitamos que todo problema a reportarse sea canalizado a la Sra. Mercedes Cordero Rosado, mediante e-mail o por escrito con copia a mi persona.

Esta es con el propósito de agilizar dichas solicitudes con la compañía que nos ofrece servicios para brindar y establecer un control de toda solicitud.

De igual forma los exhorto a utilizar de forma adecuada y responsable nuestro sistema de computadoras.

Agradezco su acostumbrada cooperación.

/mcr



COMISIÓN PARA LA
SEGURIDAD EN EL TRÁNSITO
GOBIERNO DE PUERTO RICO

A: support@sdipr.net

Control _____

FORMULARIO SOLICITUD DE SERVICIOS INFORMATICOS

Nombre: _____

Extensión: _____

Area: _____

Problema: _____

Observaciones: _____

(Especifique si ocurrió algún evento o situación que lo provocó)



Tel (787) 721-4142 Fax (787) 727-0486
www.comisionparalaseguridadeneltransito.com

Centro Gubernamental Minillas Oficina 501 Edificio Sur
Apartado 41289 Estación Minillas Santurce, Puerto Rico 00940

 **SOCIEDAD DE
LEY Y ORDEN**
GOBIERNO DE PUERTO RICO

 **Hágamos a
PUERTO RICO
VERDE**
GOBIERNO DE PUERTO RICO

Mercedes Cordero

From: Mercedes Cordero
Sent: Friday, October 07, 2011 3:16 PM
To: Abelardo Achezar; Daisy Arce; Digna Collazo; Elena Díaz; Erika Rivera Perez; Angel A. Marrero Torres; Angel L. Diaz Marrero; Felicita China; Francisca Llópez; Gisela Lorenzo; Ingrid Bofill Morales; Jannette Rodríguez Reyes; Juan R. Lopez; Kathy De Jesus; Luis M. Rosado Rosado; Luz E. Carrasquillo Valentín; Luz Marrero Rivera; Lydia Carrasquillo; Maria de L. Olivero; Maria I. Malavé; Maria Rivera; Marilu Diaz; Melvies A. Rodriguez; Milagros Santiago; Omayra Garcia; Ramon Castrillon; Tony Velazquez; Vanessa Resto; Vivian Pedraza; William Velazquez Hiraldo; Wilnerie Rivera Ortiz; Yomary Vergara
Cc: Zoriemy Rivera Hernández
Subject: SOLICITUD DE SERVICIOS DE INFORMATICA
Attachments: SOLICITUD SERV DE INFORMATICA .pdf

Buenas tardes:

Adjunto memorando relacionado a solicitud de servicios de informática.

Gracias,

Mercedes

Anejo E



COMISIÓN PARA LA
SEGURIDAD EN EL TRÁNSITO
GOBIERNO DE PUERTO RICO

Plan de
Seguridad,
Contingencia y
Recuperación

2012

Anejo F

"PLAN DE RESPUESTAS DE EMERGENCIAS Y DE RECUPERACIÓN"

Asunto: *Área de Sistemas de Información Comisión para la Seguridad en el Tránsito*

Procedimiento Núm. CST-P-10

Página 1 de 7

Fecha de efectividad
28 de diciembre de 2007

Procedimiento derogado: *N/A*

Aprobado por: *Sr. José A. Delgado Ortiz, Director Ejecutivo CST*

I. INTRODUCCIÓN:

Como parte de nuestra función primordial dentro de la Comisión para la Seguridad en el Tránsito para salvaguardar la información que se encuentra en nuestros servidores es que se crea este procedimiento.

II. BASE LEGAL:

Las disposiciones que se establecen en este procedimiento se fundamentan en la Ley Número 33 del 25 de mayo de 1972, según enmendada, Prevención de Accidentes de Tránsito, EL Programa De Prevención Anti-Corrupción de la Oficina del contralor de Puerto Rico del 8 de julio de 1988, la Ley Número 230, del 23 de julio de 1974, según enmendada, Ley de Contabilidad del Gobierno de Puerto Rico y la Ley Número 170, del 12 de agosto de 1998, según enmendada, Ley de Procedimiento Administrativo Uniforme.

III. ALCANCE:

Es obligación de todos los empleados seguir las normas y mecanismos que aquí se establecen. También será responsabilidad de ellos seguir las guías y los canales establecidos, para garantizar la corrección, legalidad, estilo y aprobación de lo que este procedimiento exponga.

IV. PROPOSITO:

Establecer una guía eficaz a seguir para tener y mantener Plan de Emergencia para los Sistemas que se encuentran en nuestros servidores.

V. CAMBIOS:

Será responsabilidad del (de la) Oficial Principal de Informática u Oficial Designado, coordinar los cambios en los procedimientos. Los cambios, no necesariamente implican que haya que cambiar el procedimiento total. Se someterán aparte y serán incluidos en el procedimiento como enmiendas.

"PLAN DE RESPUESTAS DE EMERGENCIAS Y DE RECUPERACIÓN"

Asunto: Área de Sistemas de Información Comisión para la Seguridad en el Tránsito

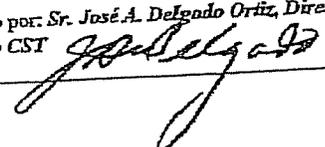
Procedimiento Núm. CST-P-10

Página 2 de 7

Fecha de efectividad
28 de diciembre de 2007

Procedimiento derogado: N/A

Aprobado por: Sr. José A. Delgado Ortiz, Director Ejecutivo CST



VI FORMULARIOS UTILIZADOS:

1. Formulario para la Prueba del Sistema de Resguardo

VII PROCEDIMIENTO:

A. Pasos para hacer resguardo y recuperación de los sistemas:

1. En cuanto a los resguardos de los sistemas como mínimo deberán cumplir con lo siguiente:
 - a. Se hará procesos de resguardos diarios, incrementales para:
 - i. Sistema Financiero (MIP)
 - ii. Sistema de Nómina
 - iii. Sistemas que corren en los servidores WINDOWS.
 - b. Semanalmente se hará un resguardo FULL de los sistemas mencionados en el paso anterior.
 - c. Mensualmente se hará un resguardo FULL a cinta de los sistemas mencionado en el punto uno y se enviará el mismo para la bóveda que se encuentra en San Patricio que se llama International Safe Deposit.
 - d. Se deben asegurar que el resguardo que se hace contenga la información deseada. Si por alguna razón en el proceso sale un error, se deben asegurar que el mismo no afecte a la información que se debe guardar.
 - e. Si por alguna razón sale un error que no logre guardar la información, se debe corregir el mismo y volver a iniciar el proceso hasta que se haga el resguardo con éxito.
 - f. Tienen que notificar a su supervisor de alguna situación que ocurra en el resguardo.
 - g. Las cintas que se envían a San Patricio tienen que estar detalladas en el Registro Resguardos Mensuales y Diarias de cintas que se envían al International Safe Deposit.

"PLAN DE RESPUESTAS DE EMERGENCIAS Y DE RECUPERACIÓN"

Asunto: *Área de Sistemas de Información Comisión para la Seguridad en el Tránsito*

Procedimiento Núm. CST-P-10

Página 3 de 7

Fecha de efectividad
28 de diciembre de 2007

Procedimiento derogado: *N/A*

Aprobado por: *Sr. José A. Delgado Ortiz, Director Ejecutivo CST*

2. Cada seis meses deben realizar una prueba de Recuperar de Cinta la información guardada para asegurarnos que el proceso está funcionando. Luego de que se haga la prueba debe llenar la Certificación en donde detalla que fue lo que recuperó y otra persona debe probar que funcione la recuperación. Esta Certificación debe ser guardada en el Archivo de la Oficina de Sistemas de Información. Adjunto se encuentra copia de la Certificación.

3. Para el mes de abril de cada año la (el) Oficial Principal de Informática se comunicará con las siguientes Agencia y/o compañías para el chequeo de los equipos necesarios para cuando ocurra una emergencia:

- a) Edificios Públicos – para que cotejen y hagan pruebas con la planta de emergencia
- b) Technical Maintenance – para que cotejen el UPS y los aires del Centro de Cómputos.
- c) Se debe verificar si están activos los contrato de mantenimiento para la red de comunicaciones
- d) Se debe verificar si están activos contrato de mantenimiento para los servidores.

B. Plan de emergencia para cuando hay Huracán o cualquier otra situación que pueda ser avisada con tiempo de antelación.

La persona que activa el Plan de Emergencia en la Agencia, luego que el Gobernador de Puerto Rico declara una emergencia, es el Director Ejecutivo de la Comisión para la Seguridad en el Tránsito.

Hay diferentes tipos de emergencias. Unas que son de imprevisto, tales como fuego, terremoto, terrorismo, etcétera. Para este tipo de emergencias, actualmente lo único que tenemos son los

"PLAN DE RESPUESTAS DE EMERGENCIAS Y DE RECUPERACIÓN"

Asunto: *Área de Sistemas de Información Comisión para la Seguridad en el Tránsito*

Procedimiento Núm. CST-P-10

Página 4 de 7

Fecha de efectividad
28 de diciembre de 2007.

Procedimiento derogado: *N/A*

Aprobado por: *Sr. José A. Delgado Ortiz, Director Ejecutivo CST*

resguardos que hacemos de los sistemas, diariamente, semanalmente y mensualmente. Los cuales son enviados a fuera de la Agencia, para que sean guardados y asegurados.

Hay otros tipos de emergencias que nos avisan con algún tiempo de antelación, tales como los huracanes. Para este tipo de situación realizaremos el siguiente proceso:

1. Cuando avisan que viene una emergencia y que hay que proteger los equipos, los administradores de los sistemas sacarán a todos los usuarios de los mismos. El (la) Oficial Principal de Informática verificará los contratos de los equipos para asegurarnos que todo está en orden y aclarar que está en contrato y que no.
2. Del Sistema Financiero (MIP) y el Sistema de Nómina se hará un backup tipo "export". Este tipo de resguardo lo que hace es guardar los datos de las aplicaciones. Si hay suficiente tiempo se hará un resguardo de la base de datos, esto se establece de esta manera, debido a que éste último resguardo tarda más de tres (3) horas en completarse y no siempre hay tanto tiempo para ejecutarlo. En los sistemas de Windows se hará un resguardo diferencial. Este tipo de resguardo guarda los cambios que han ocurrido desde el último backup realizado. Además, en los resguardos que se envían al Internacional Safe Deposit hay resguardo que contiene la base de datos y full de cada sistema, por lo que se puede recuperar la base de datos de los ya realizados.
3. Luego de que se hagan los resguardos se envían a bóveda para asegurar los datos.
4. Se procede a asegurar los equipos. Se apagan todos los equipos y si es factible se desconectan los mismos, se aseguran que no estén cerca de las ventanas. Se cubren con toldos plásticos.
5. Los directores de planificación y de administración cotejaran la lista de las personas a contactar.

"PLAN DE RESPUESTAS DE EMERGENCIAS Y DE RECUPERACIÓN"

Asunto: *Área de Sistemas de Información Comisión para la Seguridad en el Tránsito*

Procedimiento Núm. CST-P-10

Página 5 de 7

Fecha de efectividad
28 de diciembre de 2007

Procedimiento derogado: *N/A*

Aprobado por: *Sr. José A. Delgado Ortiz, Director Ejecutivo CST*

6. Después de la emergencia y luego de que se haya determinado que el edificio es seguro para entrar al mismo, los directores de planificación, administración y la Oficial Principal de Informática entran al edificio para verificar y evaluar los daños si alguno al centro. Se verifica los equipos siguiendo la hoja de cotejo, y se añadirá si se encuentra algún daño en el centro.
7. Se verifica si hay energía eléctrica, si no hay se llama a Edificios Públicos para que resuelvan la situación.
8. Si hay energía eléctrica, se verifica si se puede encender los sistemas, si no hay entonces se verifica si la planta de emergencia está activa o se puede activar. También se verificará el estatus de los equipos de comunicaciones.
9. Se verifican que suban y se corrige cualquier problema, si hay alguno.
10. Si encontramos problemas con el equipo, el (la) Oficial Principal de Informática pone una llamada de servicio a la Compañía que tiene contrato de mantenimiento.
11. Si encontramos problemas con el equipo del Sistema de Recursos Humanos y Nómina o los servidores de Windows, o cualquier otro sistema se verificará si tienen garantía, si lo tienen se llama al suplidor del contrato, si no se hace una Orden de servicio para que nos arreglen el equipo, según el procedimiento de Compra de Servicios cuando hay emergencias.
12. Como prioridad se tratará de subir primero el Sistema de Nómina, luego el sistema de Finanzas antes que el Sistema de Correo Electrónico de la Agencia o la prioridad que determine el Director Ejecutivo de la Comisión para la Seguridad en el Tránsito.

"PLAN DE RESPUESTAS DE EMERGENCIAS Y DE RECUPERACIÓN"

Asunto: *Área de Sistemas de Información Comisión para la Seguridad en el Tránsito*

Procedimiento Núm. CST-P-10

Página 6 de 7

Fecha de efectividad
28 de diciembre de 2007

Procedimiento derogado: *N/A*

Aprobado por: *Sr. José A. Delgado Ortiz, Director Ejecutivo CST*

C. Pasos a seguir luego que pasa la emergencia.

Todo aquel personal asignado para responder luego de la emergencia deberá presentarse a la Agencia, tan pronto las condiciones del tiempo lo permitan o la emergencia haya sido controlada. El personal de Sistemas de Información encargado, revisará la Hoja de Cotejo del Área de Tecnologías de Información e irá evaluando los equipos o sistemas por paso. Esta HOJA de COTEJO se conservará en la Oficina del (la) Oficial Principal de Informática. Esta Hoja de Cotejo no se somete con este procedimiento porque la misma puede cambiar tan pronto se adquiriera un equipo nuevo. Por lo que es responsabilidad del (la) Oficial Principal de Informática mantener la misma al día. Esta hoja de cotejo contendrá los equipos que hay que revisar, el estatus del mismo, la situación encontrada, si alguna, y el teléfono a contactar si el equipo está en garantía.

D. Sistemas que se levantarán luego de una emergencia para comenzar a restablecer las operaciones de la Agencia.

Los sistemas esenciales que se van a activar luego de una emergencia son los siguientes:

1. Domain Controllers, – sistemas necesarios para que se puedan conectar a los demás sistemas.
2. Sistema de Nómina – Este sistema es el que procesa y paga la nómina de los empleados de la Agencia.
3. Sistema Financiero (MIP) – Este es el sistema que contiene toda la contabilidad de la Agencia. Por el mismo se hace las certificaciones, se paga a los contratistas, etcétera.
4. Sistema FASGO – Este es el sistema que trabaja con los activos de la agencia.
5. Sistema de Correo Electrónico - Este sistema es el que corre el correo electrónico de la Agencia. Este sistema es el último que se levantará luego de que estén arriba los antes mencionados.

"PLAN DE RESPUESTAS DE EMERGENCIAS Y DE RECUPERACIÓN"

Asunto: *Área de Sistemas de Información Comisión para la Seguridad en el Tránsito*

Procedimiento Núm. CST-P-10

Página 7 de 7

Fecha de efectividad
28 de diciembre de 2007

Procedimiento derogado: *N/A*

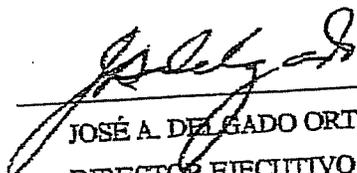
Aprobado por: *Sr. José A. Delgado Ortiz, Director Ejecutivo CST*

VIII. ENMIENDAS:

Las enmiendas a este procedimiento serán procesadas a través de la Oficina de Sistemas de Información y aprobadas por el Director Ejecutivo.

IX. VIGENCIA:

Las disposiciones promulgadas en este Procedimiento comenzarán a regir inmediatamente después de su aprobación y derogan cualquier norma o disposición en conflicto con las mismas.



JOSÉ A. DELGADO ORTIZ
DIRECTOR EJECUTIVO

28 de diciembre de 2007

FECHA

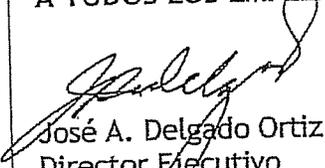
Anejo H



Año Fiscal 2006-2007
22 de junio de 2007

Memorando Circular
CST-07-05

A TODOS LOS EMPLEADOS


José A. Delgado Ortiz
Director Ejecutivo

POLÍTICA SOBRE EL USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y CORREOS ELECTRÓNICOS

Con el propósito de cumplir con las recomendaciones de los informes de auditoría de la Oficina del Contralor de Puerto Rico, la Oficial Principal de Informática y la Auditora Interna de la CST estarán estableciendo los controles necesarios para garantizar el uso eficiente del acceso al Internet y al correo electrónico de los sistemas Tecnológicos de Información

A tales efectos, la oficial Principal de Informática d la CST, Sra. Rosa Marcano, confeccionó la Política sobre el Uso de Sistemas de Información, de la Internet y Corres Electrónicos que se acompaña en este Memorando bajo la Codificación CST-POL-02.

Este Memorando Circular deroga el comunicado por e-mail enviado el 20 de junio de 2005 y la Política sobre el Uso de Sistema de Información, de la Internet y Correo Electrónicos del 16 de junio de 2005.

Será responsabilidad de cada supervisor hacer cumplir la política con respecto al uso adecuado de estos sistemas computarizados. Cualquier empleado que viole las disposiciones relacionados con los mismos, podrá ser sancionado conforme a las penalidades establecidas en el "Manual de Normas de Conducta y Medidas Disciplinarias" de la CST.

Cuento con su acostumbrada cooperación para mejorar la fiscalización y uso de los fondos públicos.

Anejo G



COMISIÓN PARA LA
SEGURIDAD EN EL TRÁNSITO
GOBIERNO DE PUERTO RICO

Informe de Configuración Sistemas de Informática

Comisión para la Seguridad en el Tránsito
Puerto Rico

Agosto 2012

Anejo I

“POLÍTICA SOBRE EL USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y CORREOS ELECTRÓNICOS”

Asunto: Área de Sistemas de Información, *Comisión para la Seguridad en el Tránsito*

Política Núm. CST-POL-02

Página 1 de 3

Fecha de efectividad
de _____ de 200_

Procedimiento derogado:
Correo electrónico del 20 de junio de 2005 y Política sobre el uso de Sistemas de Información, de la Internet y Correos Electrónicos del 16 de junio de 2005.

Aprobado por: *José A. Delgado Ortiz*, Director Ejecutivo

Normas Generales Aplicables al Uso de Sistemas de Información

Esta política define el uso aceptable de los Sistemas de información de la Comisión para la Seguridad en el Tránsito. De esta manera protegemos al usuario y al Gobierno del Estado Libre Asociado de Puerto Rico de posibles situaciones que pongan en peligro los sistemas y la información que contienen.

Estas políticas están basadas en Información suministrada por la Oficina de Gerencia y presupuesto específicamente de Tecnologías de Información Gubernamental. Conforme a esto, es necesario establecer las políticas necesarias para garantizar el uso adecuado de los sistemas de información.

Todos los empleados deberán firmar esta política sin excepciones comprometiéndose a cumplir con las mismas. El incumplimiento de estas políticas podría conllevar multas y sanciones severas.

Se prohíbe la instalación de programas no autorizados por la OGP o la CST aunque sean libres de costo. La información desarrollada, transmitida o almacenada es propiedad de la CST y del Estado Libre Asociado de Puerto Rico. La información brindada sin la autorización esta totalmente prohibida, así como también es responsabilidad del empleado salvaguardar la confidencialidad de los datos.

Se prohíbe además el compartir claves de acceso a los diferentes sistemas. El acceso una cuenta ajena sin autorización esta totalmente prohibido, por lo que esta acción se castigara conforme a la legislación local y federal vigentes. Cada usuario será individualmente responsable por el manejo adecuado de los códigos no impedirá que los sistemas o programas en la computadora asignada para su uso sea auditada para garantizar que se poseen todas las licencias requeridas.

Se prohíbe el uso de material que discrimine por razón de género, raza, condición social, económica y física, origen nacional, ciudadanía, ideas políticas, o cualquier otro criterio prohibido por ley o por la Constitución.

Los recursos informáticos de la CST no se usaran para propósito alguno que sea ilícito o contrario a las normas, reglamentos y políticas establecidas por ley.

Normas Generales Aplicables al Uso de Internet

Los sistemas de comunicación y acceso al Internet son propiedad de la CST y deberán ser utilizados exclusivamente como herramienta de trabajo conforme a las normas que rigen el comportamiento personal de la entidad y nunca con fines no oficiales o personales o con fines de lucro.

"POLÍTICA SOBRE EL USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y CORREOS ELECTRÓNICOS"

Asunto: Área de Sistemas de Información, Comisión para la Seguridad en el Tránsito

Política Núm. CST-POL-02

Página 2 de 3

Fecha de efectividad
de _____ de 200_

Procedimiento derogado:
Correo electrónico del 20 de junio de 2005 y Política sobre el uso de Sistemas de Información, de la Internet y Correos Electrónicos del 16 de junio de 2005.

Aprobado por: *José A. Delgado Ortiz*, Director Ejecutivo

Las operaciones realizadas a través del Internet no tienen expectativa de privacidad referente al uso y accesos realizados; por lo cual la agencia tiene el derecho de intervenir y auditar los accesos realizados por los usuarios y a su contenido.

Normas Generales Aplicables al Uso de Correos Electrónicos

El sistema de correo electrónico es propiedad de la CST por lo que tiene la autoridad y el derecho absoluto de intervenir, auditar e investigar para mantener un control adecuado del mismo sin la previa autorización del usuario.

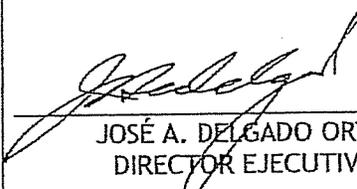
El correo electrónico podrá utilizarse únicamente para propósitos relativos a las funciones de la Comisión. Se prohíbe el uso de asuntos no oficiales o actividades personales con fines de lucro. No deberán utilizarse para uso personal; ni para transmitir, acceder o almacenar comunicados que sean discriminatorios, ofensivos, profanos, obscenos o vayan en contra de las buenas costumbres o de las leyes.

Se prohíbe obtener acceso no autorizado a las cuentas de correo electrónico, a leer, interceptar o revisar cualquier documento electrónico sin el consentimiento del remitente y del destinatario de la comunicación.

En adición, se prohíbe todo tipo de hostigamiento, discrimen o intimidación. No se tolerara mensajes o comentarios despectivo alguno sobre raza, edad, genero, estado civil, linaje, limitación física o mental, religión, ni de origen nacional o étnico, tampoco sobre atributos físicos o preferencias sexuales, credos políticos de un individuo p grupo de individuos.

Durante horas laborables, los usuarios no podrán utilizar o acceder a cuentas de correo electrónico distintas a las cuentas oficiales de la comisión, a menos que estén autorizados por escrito a tal uso.

Esta política entrará en vigor una vez sea firmada por el Director Ejecutivo



JOSÉ A. DELGADO ORTIZ
DIRECTOR EJECUTIVO

25 de junio de 2007

FECHA

“POLÍTICA SOBRE EL USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y CORREOS ELECTRÓNICOS”

Asunto: Área de Sistemas de Información, *Comisión para la Seguridad en el Tránsito*

Política Núm. CST-POL-02

Página 3 de 3

Fecha de efectividad
_ de _ de 200_

Procedimiento derogado:
Correo electrónico del 20 de junio de 2005 y Política sobre el uso de Sistemas de Información, de la Internet y Correos Electrónicos del 16 de junio de 2005.

Aprobado por: *José A. Delgado Ortiz*, Director Ejecutivo

CUMPLIMIENTO DE LA POLÍTICA

El no cumplir con las políticas establecidas y relacionadas a los sistemas de información podría conllevar sanciones y/o suspensión del empleado.

Certifico que he leído y entendido este documento y reconozco que pasara a ser parte de mi expediente de personal; por lo cual mediante mi firma me comprometo a cumplir con las mismas.

Nombre del Empleado

Posición ó Puesto

Firma del Empleado

Fecha

Anejo J

Anejo K

COMISION PARA LA SEGURIDAD EN EL TRANSITO

ENTREGA, RECIBO Y SALIDA DE "TAPES"
"BACKUP" SISTEMA DE INFORMATICA

Periodo del ___ de _____ al ___ de _____ de 20__

Técnico Contratado Sistema de Información

Hago entrega de los siguientes "tapes" con la información suministrada a través de los "backup" de los servidores.

- (a) _____ (b) _____ (c) _____ (d) _____
(e) _____ (f) _____ (g) _____ (h) _____

Información de los "tapes": _____

Entregado por: _____
Nombre del Consultor

Firma: _____

Fecha: _____

Empleado de la Agencia

Certifico que recibí los "tapes", enumerados en este documento, para ser enviados a la bóveda de la Compañía International Safe Deposit & Courier Services Corp.

Recibido por: _____

Firma: _____

Fecha: _____

.....
Servicio de Acarreo

Certifico que recibí los "tapes" enumerados en este documento con el propósito de brindar el servicio de Acarreo contratado.

Recogido por: _____
International Safe Deposit

Firma: _____

Fecha: _____

Area de Documentos de la Agencia

Certifico que recibí copia de este documento.

Firma: Administradora de Documentos

Fecha

Anejo L

CONTRATO - ACARREO DE DATA ELECTRONICA

DE UNA PARTE: INTERNATIONAL SAFE DEPOSIT & COURIER SERVICES CORPORATION, una corporación organizada en conformidad con las Leyes del Estado Libre Asociado de Puerto Rico, en adelante denominada "ISD&CSC", y de OTRA PARTE:

COMISION PARA LA SEGURIDAD EN EL TRANSITO
(En adelante denominado "CLIENTE")

Espacio: C-23

Acuerdan lo siguiente:

1. TÉRMINOS Y CONDICIONES PARA ACARREO DE DATA ELECTRÓNICA

- A. ISD&CSC proveerá servicio de acarreo durante la vigencia de este contrato al CLIENTE, de artículos tales como: "tapes" de computadoras, cartridges, discos compactos (CD), películas, negativos, estuches de almacenaje, maletas, envases y otros medios y equipo para el almacenaje de data electrónica, magnética o fotográfica, denominado de aquí en adelante en términos genéricos como DATA. La misma será entregada por el CLIENTE a ISD&CSC, o recogida por esta en envases adecuados para la transportación y manejo de la DATA.
- B. El CLIENTE tiene que haber suscrito con ISD&CSC un contrato de alquiler de espacio para el almacenaje de DATA.
- C. El servicio de acarreo se dará dentro de nuestro itinerario diario. Entregaremos en: Centro Gubernamental Minillas, Ofic. 501, Edif. Sur. y luego de visitar todas las compañías programadas, se regresa a la Bóveda de ISD&CSC.
- D. El CLIENTE cederá a ISD&CSC una, de las dos únicas llaves existentes, para poder tener acceso al espacio. Al momento de una cancelación del acarreo, ISD&CSC devolverá la llave al CLIENTE. En caso de que el CLIENTE cancele también el alquiler del espacio, el CLIENTE devolverá su llave a ISD&CSC.
- E. Toda maleta, envase o paquete entregado a ISD&CSC para ser almacenado estará clara y conspicuamente rotulado para su identificación y manejo. En caso de que el CLIENTE no provea maletas para el manejo de su DATA, ISD&CSC lo adquirirá y facturará el costo al CLIENTE, el cual accede a pagar al serie facturado.
- F. ISD&CSC hará un inventario mensual de todo lo guardado en el espacio alquilado, y se le enviará al CLIENTE vía correo electrónico a la siguiente dirección: mcordero@cst.gobierno.pr; midrach@cst.gobierno.pr

2. CARGOS Y SERVICIOS

- A. Todos los cargos de acarreo están calculados por recorridos completos (ida y vuelta) bajo itinerarios preestablecidos. El CLIENTE pagará a ISD&CSC \$24.00 por cada viaje de acarreo que se provea.
- B. Servicios especiales tendrán un costo extra. Estos servicios especiales son los que el CLIENTE pide en días laborables después de las 9:30 a.m., y lo necesita para el mismo día. Si el pago es por Orden de Compra, favor de añadir varios servicios extras para que los puedan cubrir.
- C. El servicio de acarreo estará disponible durante el (o los) días que las partes acuerden que será: 2do. viernes de mes.
- D. ISD&CSC proveerá servicio de acarreo en otros días no acordados siempre y cuando el CLIENTE lo solicite con suficiente tiempo de antelación, para que ISD&CSC pueda coordinar dicho servicio.
- D. Los servicios rendidos serán pagados por el CLIENTE a ISD&CSC cada mes de servicio, al momento de recibir la factura correspondiente, la cual es pagadera a su presentación.

3. TERMINO: La vigencia de este contrato será por el término de 1 año.

4. RETIRO Y ENTREGA DE DATA

- A. Cuando el CLIENTE o su representante autorizado requiera el recogido o entrega de la DATA, dará a ISD&CSC un tiempo razonable para ello. No aseguramos una hora en específico. En la eventualidad de que ISD&CSC no pueda cumplir con las condiciones de este acuerdo por razón de fuerza mayor, que puede incluir sin limitación alguna, actos de Dios, inundaciones, guerra, epidemias, enemigos públicos, dictámenes de corte, disposiciones de ley, regulaciones u ordenanzas gubernamentales, huelgas, disturbios civiles, fallas en equipo, o cualquier otra condición que esté más allá del control de ISD&CSC, o por la pérdida o destrucción de la data por cualesquiera de las condiciones antes señaladas, ISD&CSC no será responsable por el incumplimiento y/o daños sufridos.
- B. El CLIENTE se compromete a seguir el Plan de Contingencia establecido por ISD&CSC en caso de desastres como terremotos, huelgas, inundaciones o huracán. El mismo está publicado en nuestra página web: internacional-safe.com.
- C. ISD&CSC, a su sola discreción, determinará la aceptación de la DATA a almacenarse y podrá rechazar cualquier DATA que en su opinión no reúna los requisitos mínimos de aceptación que de tiempo en tiempo puedan ser implementados por ISD&CSC. ISD&CSC no será responsable, ni asume responsabilidad alguna, por la identificación incorrecta de la DATA, su contenido o condición. Al recibo y entrega de cualquier DATA, ISD&CSC expedirá un Certificado de Recibo describiendo el material recibido por el CLIENTE. El CLIENTE firmará dicho recibo haciendo constar que tal DATA ha sido presentada en la misma condición en la cual fue entregada a ISD&CSC. ISD&CSC entregará la DATA al personal autorizado a recibir la misma por el CLIENTE. El CLIENTE examinará la DATA entregada por ISD&CSC al momento de su entrega para determinar la condición de la misma. El Certificado de Recibo será evidencia de que todo se ha recibido en orden y libera a ISD&CSC de cualquier reclamación que el CLIENTE pueda tener sobre esa entrega.

5. Todos los términos y condiciones del "Contrato de Almacenaje de DATA Electrónica", suscrito entre ISD&CSC y el CLIENTE, se incorporan y se hacen formar parte de este contrato.

En testimonio de lo cual las partes firman el presente acuerdo hoy 29 de Septiembre de 2011 1 de Octubre de 2011.

CLIENTE

Zoriemy Rivera Hernández, Directora Ejecutiva
Firma Autorizada

International Safe Deposit & Courier Services Corp

[Firma]
Gerente

Comisión Seg. en el Tránsito
Cliente: 3071

Contrato: 4605

Anejo 0



COMISION
PARA LA SEGURIDAD
EN EL TRANSITO

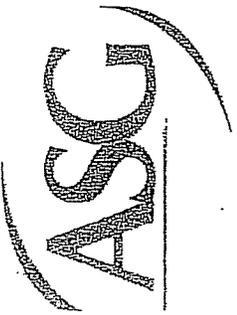
PO Box 41289
San Juan PR 00940-1289

DESCRIPCION DEL PUESTO

1.	Apellido Paterno VELAZQUEZ	Apellido Materno o del Esposo Hiraldo	Nombre e Inicial William	5.	Título Funcional del Puesto Auxiliar Administrativo
2.	Número de Seguro Social n/a	Número del Puesto n/a		6.	Oficina, División y Sección Administración
4.		Título de Clasificación del Puesto Auxiliar Administrativo		7.	Teléfono y extensión (707) 721-1142 Ext. 2194

8. Detalle las funciones esenciales y marginales que usted realiza en el orden de importancia de las mismas, comenzando con la más importante. Indique el tiempo que dedica a cada una en porcentaje del total del tiempo que dedica a su puesto. **ESTA ES LA PARTE MAS IMPORTANTE DEL FORMULARIO.** Use sus propias palabras y haga las descripciones de sus deberes tan claras que personas que no estén tan familiarizadas con su trabajo entiendan con exactitud lo que usted hace. Las funciones marginales deberán identificarse como tales al finalizar el detalle de las funciones esenciales.

TIEMPO	FUNCIONES DEL PUESTO	NO LLENE ESTE ESPACIO
	<p>ESENCIALES</p> <ol style="list-style-type: none"> Mantiene bajo su custodia, cuidado y protección la conservación y uso adecuado de toda la propiedad de la GST como Encargado de la Propiedad mediante delegación expresa del Director Ejecutivo. Verifica el número de propiedad para los activos fijos adquiridos en el sistema FAS GOV y los registra en los Informes de Recibo e Inspección. Prepara el Recibo por Propiedad en Uso (Modelo SC 1211), imprime el sello de goma con número de propiedad y luego marca el equipo de tres (3) maneras diferentes: barra electrónica, lápiz electrónico y/o marcador negro. Prepara el Informe de Enmienda al Activo Fijo (Modelo SC 785) para las solicitudes de donación y/o transferencia en conjunto con las agencias y las instituciones que lo solicitan y los tramita al Departamento de Hacienda para que se realice la baja o corrección en nuestro inventario de activos fijos. Procesa la Declaración de Propiedad Excedente (Modelo SC 787) y envía al Departamento de Hacienda de ser requerido. Hace un inventario completo del equipo a decomisarse y coordina con la Compañía o Institución el recogido del mismo. Prepara el Informe de Pérdida de Propiedad, Bienes o Fondos Públicos (OC-10-04) para informar a la Oficina del Contralor y/o el Secretario de Justicia de los casos de activos fijos perdidos o robados. Mantiene un suministro apropiado de materiales y prepara la Solicitud de Compras y Servicios para la firma del Director cuando sea necesario comprar materiales. 	



GOBIERNO DE PUERTO RICO
ADMINISTRACION DE SERVICIOS GENERALES



CERTIFICADO DE PARTICIPACIÓN
OTORGADO A

WILLIAM VELAZQUEZ HIRALDO

Por haber participado en el Adiestramiento para:

Procedimientos para Declarar la Propiedad Excedente
en las Agencias del Gobierno de Puerto Rico

En cumplimiento Ley 164 del 23 de julio de 1974,
Reglamento #9

Expedido en San Juan, Puerto Rico, hoy 8 de septiembre de 2011

CARLOS E. VÁZQUEZ PESQUERA
ADMINISTRADOR

Kerr Consulting & Support – Puerto Rico

1510 Ponce de León Avenue, San Juan, PR 00909

Certificate of Completion

This certificate is presented to

William Velázquez Hiraldo

For successfully completing

FAS Gov Asset Accounting Training

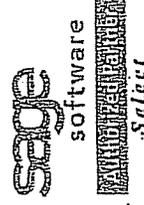
Date: August 14-15, 2012 **Location:** San Juan, PR

Category: Technical Accounting – 16 credits

*CPE credits have been granted based on 50 – minute contact hour
Instructional Delivery Method: Group - Live*

A Hernández E.

Authorized Signature



Anejo N

Anejo M

Angel L. Diaz Marrero

From: Kenny Monell [kmonell@sdipr.net]
Sent: Tuesday, September 11, 2012 8:21 PM
To: Angel L. Diaz Marrero; Jannette Rodriguez Reyes; Zoriemy Rivera Hernández; Milagros Santiago
Subject: SDI: Reporte de Inventario de Programas
Attachments: Installed_Applications_2012-09-11.xls

Saludos Angel;

Adjunto Reporte de Inventario de Programas segun solicitados.

Gracias.

--

Atentamente,

--

Kenny Monell
Technical Support
Software Development International
District View Plaza, Suite 301
644 Fernandez Juncos Ave.
San Juan, P.R. 00907-3122
www.sdipr.net
kmonell@sdipr.net
Tel.787.919.7314
Fax 866.532.7786

Please consider the environment and do not print this e-mail unless you really need to.

CONFIDENTIALITY NOTE:

This e-mail and any attachments are confidential and may be protected by legal privilege. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of this e-mail or any attachment is prohibited. If you have received this e-mail in error, please notify us immediately by returning it to the sender and delete this copy from your system. Thank you for your cooperation.

CST: Installed Applications
 Summary of all applications installed
 597 Items.
 Sep 11, 2012

Application	Number of	Oldest Ver:	Latest Version
2007 W-2	1	1.0.100	1.0.100
2008 W-2	1	1.0.0	1.0.0
2009 W-2	1	1.0.0	1.0.0
2010 W-2	2	1.0.0	1.0.0
2011 W-2	2	1.0.0	1.0.0
32 Bit HP C3		2.1.4	6.1.2
3Com Devi 1		1.0.0.0	1.0.0.0
3D Tropica 1		1.0	1.0
5300_5400 1		1.00.0000	1.00.0000
5300_5400 1		1.00.0000	1.00.0000
7-Zip	1	9.20	9.20
7500_7600 2		1.00.0000	1.00.0000
A30 Comm 1		1.1.0.6	1.1.0.6
Accelerome 1		2.00.10.33	2.00.10.33
Acrobat.co 9		0.0.0	1.7.258
ActivClient 2		6.01.0003	6.01.00034
ADM files fi 1		1.0.10	1.0.10
Adobe Acrc 2		4.0	5.0
Adobe AIR 10		1.0.8.4990	2.0.3.13070
Adobe Dow 2		2.0	2.0
Adobe Flas 1		9	9
Adobe Flas 7		10.0.32.18	10.3.183.7
Adobe Flas 2		10.0.22.87	10.0.22.87
Adobe Flas 3		11.1.102.5	11.3.300.265
Adobe Flas 2		9.0.124.0	9.0.124.0
Adobe Rea 10		7.0.5	9.5.0
Adobe Rea 5		10.1.1	10.1.3
Adobe Sho 1		11.6.3.633	11.6.3.633
Adobe@ Pf 2		3.00.000	3.00.000
Agere Syst 3			
ALPS Toucl 1			
AOL Toolba 1		5.2.69.1	5.2.69.1
APC Power 1		2.0	2.0
Aplicación 1			
ASAP Utilit 1		4.6.0	4.6.0
ATI Cataly 1		3.0.664.0	3.0.664.0
ATI Display 3		8.19.4-0518	8.19.4-051206a-031537C-IBM
AuthenTec 1		8.4.4.20	8.4.4.20
AuthenTec 1		8.0.26.34	8.0.26.34
Bing Bar 2		5.0.1449.0	7.0.765.0
Bing Bar Pl 1		5.0.1449.0	5.0.1449.0
BioAPI Frar 1		1.0.2	1.0.2
BIOS Confi 1		4.00 A7	4.00 A7

CCC Help K 1	2008.0508	2008.0508.2150.37248
CCC Help M 1	2008.0508	2008.0508.2150.37248
CCC Help F 1	2008.0508	2008.0508.2150.37248
CCC Help F 1	2008.0508	2008.0508.2150.37248
CCC Help F 1	2008.0508	2008.0508.2150.37248
CCC Help S 1	2008.0508	2008.0508.2150.37248
CCC Help S 1	2008.0508	2008.0508.2150.37248
CCC Help T 1	2008.0508	2008.0508.2150.37248
CCC Help T 1	2008.0508	2008.0508.2150.37248
ccc-core-st 1	2008.0508	2008.0508.2151.37248
ccc-utility 1	2008.0508	2008.0508.2151.37248
CCleaner 4	3.12	3.21
Choice Guæ 1	1.2.87.0	1.2.87.0
Cisco EAP-I 1	2.2.14	2.2.14
Cisco LEAP 1	1.0.19	1.0.19
Cisco PEAP 1	1.1.6	1.1.6
Compaq Ræ 1		
Compatibil 5	12.0.6021.	12.0.6425.1000
Conexant [1		
Corel Appli 1		
Credential 2	4.0.3.1208	4.0.3.1208
Crystal Ref 2	12.2.0.290	12.2.0.290
Curso Inter 1	1.01.0000	1.01.0000
Custom 1	01.00.00.0	01.00.00.000
CustomerR 1	1.00.0000	1.00.0000
CutePDF W 1	2.7	2.7
CyberLink l 1	9.5.1.4418	9.5.1.4418
D3DX10 2	15.4.2368.	15.4.2368.0902
Definition l 1		
Dell Backu 1	1.3.1	1.3.1
Dell Client 1	1.2.1	1.2.1
Dell Data F 2	2.1.00001.	2.1.00001.001
Dell Data F 1	2.01.018	2.01.018
Dell Data F 1	2.01.010	2.01.010
Dell Edoc v 1	1.0.0	1.0.0
Dell Featur 1	2.1.000	2.1.000
Dell OpenM 1	5.5.0	5.5.0
Dell Resou 1		
Dell SAS R. 2	2.08.0000	2.08.0000
Dell Touch 1	7.1208.10:	7.1208.101.125
Dell Webca 1	1.40.28	1.40.28
DellAccess 1	01.00.00.1	01.00.00.108
Destinator 2	130.0.0.0	130.0.0.0
DeviceDisc 2	140.0.213.	140.0.213.000
DeviceMan 1	1.00.0000	1.00.0000
Digital Line 2	1.14	1.21
DirectX 9 F 1	1.00.0000	1.00.0000
DiskPie 1	2.1	2.1
DocProc 2	140.0.100.	140.0.100.000

DocProcQF 1	1.00.0000	1.00.0000
Drive Encry 2	4.0.2	4.0.2
DTOP Devir 1	1.0	1.0
DW WLAN 1	5.100.235.	5.100.235.13
eBay Icon 1	1.0	1.0
EMBASSY 1	04.02.00.1	04.02.00.173
ESU for Mik 2	1.00.1.3	1.00.2.1
eSupportQ 1	1.00.0000	1.00.0000
FAS Gov 1(5	2008.1	2008.1
FAS Gov 1(1	8.1	8.1
FAS Gov 1(1	2008.1	2008.1
FAS Report 4	8.5.0.2175	8.5.0.2175
Fatal Reflex 1	3	3
Fax 2	140.0.213.	140.0.213.000
File Sanitiz 2	1.0.0.16	1.0.0.18
File Scaver 1	3.2	3.2
FreeUndele 1		
Gemalto 1	01.01.01.0	01.01.01.0000
Google Chr 1	20.0.1132.	20.0.1132.57
Google Ear 2	5.2.0.5920	6.1.0.5001
Google Toc 4	1.0.0	7.3.2710.138
Google Upc 3	1.3.21.115	1.3.21.115
GPBaseSer 1	140.0.212.	140.0.212.000
Hewlett-Pa 2	1.1.15.2	1.1.15.2
Hewlett-Pa 2	2.0.63.2	2.0.63.2
HijackThis 1	2.0.2	2.0.2
HP 3D Driv 2	3.10 A7	3.10 A7
HP Active 2	3.1.4.1	3.1.4.1
HP Array C 1		
HP Custom 2	5.4.0.2423	5.4.0.2423
HP Custom 3	7.0	14.0
hp deskjet 3	1.01.0000	1.01.0000
hp deskjet 3		
HP Doc Vie 2	1.03.0001	1.03.0001
HP Easy Se 2	5.4.0.2423	5.4.0.2423
HP Help an 2	2.0.8.0	2.0.9.0
HP Imaginç 2	7.0	14.0
HP Insight 1		
HP Insight 1		
HP Integra 2	6.0.1.6200	6.0.1.6200
HP JavaCal 2	04.00.01.0	04.00.01.0025
hp LaserJet 2	1000	1000
hp LaserJet 1		
HP OfficeJe 2	14.0	14.0
HP Officeje 1	1.0	1.0
HP Officeje 2	1.3	1.5
HP Photosr 1	1.12.0.46	1.12.0.46
hp print sc 1		
HP Product 3	9.7.3	10.7.9.0

HP ProLian	1		
HP Protect	2	4.00 A1A	4.00 A1A
HP Protect	2	04.00.01.0	04.00.01.0026
HP Quick L	2	6.40 D3	6.40 E1
HP QuickLc	1	2.0.0.6	2.0.0.6
HP Smart \	2	4.60	4.60
HP Softwar	2	5.00.A.5	5.00.A.7
HP Solutior	2	7.0	14.0
HP Total C:	1	2.1.3564.2	2.1.3564.2652
HP Update	5	4.000.010.	5.003.001.001
HP User Gl	2	1.01.0000	1.03.0000
HP Version	1	2.0	2.0
HP Wallpaç	1	1.0.1.4	1.0.1.4
HP Webcar	2	5.8.39004.	5.8.39004.0
HP Webcar	2	1.0.020.04	1.0.020.0418
HP Wireles:	2	3.00 J1	3.00 K1
HPDiagnos	1	1.00.0000	1.00.0000
HPNetwork	2	1.1.70	1.1.70
HPProduct/	2	70.0.170.0	140.0.213.000
HPSSupply	3	100.0.172.	140.0.212.000
Hypercom	1	1.2.007	1.2.007
IDEA	1	7.2.0	7.2.0
IIS 6.0 Res	1	6.00.0000	6.00.0000
IncrediMail	1	5.8.6.4184	5.8.6.4184
Intel(R) Gr	7	6.14.10.45	8.15.10.1930
Intel(R) Id	1	1.1.2.0	1.1.2.0
Intel(R) M	1	7.0.0.1144	7.0.0.1144
Intel(R) M	1		
Intel(R) Ne	3	13.1.33.0	13.1.33.0
Intel(R) Pri	1	8.15.10.24	8.15.10.2418
Intel(R) PR	2	9.00.0000	11.01.0000
Intel® Mat	2		
Internal Ne	1	1.7.0	1.7.0
InterVideo	2		
InterVideo	2	1.0.4.0	1.0.4.0
InterVideo	2	5.0-B11.12	5.0-B11.1248
IPMI Drive	3	1.00.0000	1.00.0000
Java Auto	14	2.0.2.1	2.1.5.1
Java Runtii	4	1.4.2_03	1.5.0.120
Java(TM)	69	1.6.0.30	6.0.240
Java(TM)	71	7.0.10	7.0.10
Junk Mail f	1	15.4.3502.	15.4.3502.0922
K5400	1	50.0.165.0	50.0.165.000
L7700	2	140.0.000.	140.0.000.000
LAN-Fax UI	6		
LaserAIO	1	1.00.0000	1.00.0000
Lexmark	1:1		
Lexmark S:	8		
LightScribe	3	1.12.29.2	1.12.37.1

LiveReg 1	2.2.0.1621	2.2.0.1621
LiveUpdate 18	2.0.39.0	3.3.0.92
Living 3D v1	1.0	1.0
LogMeIn 1	4.1.1558	4.1.1558
ManageEnç 1	9.0	9.0
MarketResç 3	70.0.170.0	140.0.214.000
mCore 2	1.19.0000	9.03.0000
mDriver 1	9.03.0000	9.03.0000
mDrWiFi 2	1.19.0000	9.03.0000
MediaFACE 1	4.0	4.0
Mesh Runti 1	15.4.5722.	15.4.5722.2
mHelp 1	9.03.0000	9.03.0000
mHlpDell 1	1.19.0000	1.19.0000
Microsoft .I 9	1.1.4322	3.5.21022
Microsoft .I 2	1.1.4322	4.0
Microsoft .I 14	KB241644;	KB979906
Microsoft .I 13	2	2.2.30729
Microsoft .I 9	2	3.2.30729
Microsoft .I 9	3.5.30729	3.5.30729
Microsoft .I 7	4.0.30319	4.0.30319
Microsoft .I 6	4.0.30319	4.0.30319
Microsoft A 6	11.0.5228.	12.0.6012.5000
Microsoft A 19	1.0.1979.0	1.0.1979.0
Microsoft B 2	2.0.6706.0	2.2.2170
Microsoft C 2	1	1
Microsoft D 1	2.1.55.0	2.1.55.0
Microsoft E 1	2003	2003
Microsoft E 1	6.5.7926.0	6.5.7926.0
Microsoft G 1	1.0.2.0	1.0.2.0
Microsoft H 8		
Microsoft I: 1	2006	2006
Microsoft I: 1	1	1
Microsoft I: 1		
Microsoft K 2	1.5	1.7
Microsoft L 1	1.40.164.0	1.40.164.0
Microsoft N 8		
Microsoft C 9	11.0.5614.	2003
Microsoft C 1	11.0.8173.	11.0.8173.0
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 6	12.0.4518.	2007
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.6425.1000
Microsoft C 3	12.0.4518.	12.0.4518.1014

Microsoft C 3	12.0.4518.12.0.6425.1000
Microsoft C 1	2007 2007
Microsoft C 3	12.0.4518.12.0.6425.1000
Microsoft C 3	12.0.4518.12.0.6425.1000
Microsoft C 3	12.0.4518.12.0.6425.1000
Microsoft C 1	14.0.4763.14.0.4763.1000
Microsoft C 8	14.0.4763.14.0.6029.1000
Microsoft C 9	14.0.4763.2010
Microsoft C 8	14.0.4763.14.0.6029.1000
Microsoft C 1	2010 2010
Microsoft C 8	14.0.4763.14.0.6029.1000
Microsoft C 8	14.0.4763.14.0.6029.1000
Microsoft C 8	14.0.4763.14.0.6029.1000
Microsoft C 1	12.0.4518.12.0.4518.1031
Microsoft C 1	2.0.2313.0 2.0.2313.0
Microsoft C 1	2.0.4024.1 2.0.4024.1
Microsoft C 2	12.0.6414.14.0.5118.5000
Microsoft C 1	
Microsoft C 1	1.0.0.0 1.0.0.0
Microsoft C 1	2.7 2.7
Microsoft C 19	2.0.591.0 2.0.591.0
Microsoft C 19	1.0.1979.0 2.0.684.0
Microsoft C 19	2.0.585.0 2.0.585.0
Microsoft P 1	1.1.0.3463 1.1.0.3463
Microsoft P 19	1.3.3555.0 1.3.3555.0
Microsoft R 4	8.0.56405 2005
Microsoft S 2	1.3.59.0 3.0.133.0
Microsoft S 4	3.0.50106.4.1.10329.0
Microsoft S 7	12.0.4518.14.0.4763.1000
Microsoft S 3	2000 2005
Microsoft S 7	8.05.2004 8.05.2312
Microsoft S 1	9.00.3104 9.00.3104
Microsoft S 3	3.1.0000 3.1.0000
Microsoft S 1	9.4.5000.0 9.4.5000.00
Microsoft S 2	9.2.3042.0 9.4.5000.00
Microsoft S 1	
Microsoft S 1	9.00.3042.9.00.3042.00
Microsoft S 2	9.00.3042.9.00.5000.00

Microsoft S 2	9.00.3042.9.00.5000.00
Microsoft S 2	9.00.3042.9.00.5000.00
Microsoft U 2	1.0 1.0
Microsoft V 2	8.0.50727.8.0.50727.4053
Microsoft V 13	8.0.50727.8.0.61001
Microsoft V 1	9.0.30729.9.0.30729.4148
Microsoft V 11	9.0.21022 9.0.30729.6161
Microsoft V 6	10.0.30319 10.0.30319
Microsoft V 1	8.0.50727.8.0.50727.42
Microsoft X 3	8.40.9419.8.50.2162.6
Microsoft X 1	4.10.9404.4.10.9404.0
MIP Sampl 1	6.2.0.0 6.2.0.0
Misc 2	1.00.0000 1.00.0000
mIWA 2	1.19.0000 9.03.0000
mIWCA 1	1.19.0000 1.19.0000
mLogView 2	1.19.0000 9.03.0000
mMHouse 2	1.19.0000 9.03.0000
Modem Dia 1	1.0.28.0 1.0.28.0
Modem Hel 1	2.41 2.41
MotoHelper 1	1.2.0 1.2.0
Mozilla Fire 1	3.0.5 (en-l 3.0.5 (en-US)
mPFMgr 2	1.19.0000 9.03.0000
mPFWiz 2	1.19.0000 9.03.0000
MPM 3	1.00.0000 1.00.0000
mProSafe 2	9.00.0000 9.00.0000
mSCfg 1	9.03.0000 9.03.0000
MSN 1	
MSN Music 1	
mSSO 1	1.19.0000 1.19.0000
MSVCRT 3	14.0.1468.15.4.2862.0708
MSXML 4.0 38	4.20.9841.4.20.9876.0
MSXML 6 S 6	6.20.2003.6.20.2003.0
MSXML 6.0 1	6.10.1129.6.10.1129.0
mToolkit 1	1.19.0000 1.19.0000
mWlsSafe 2	9.00.0000 9.00.0000
mXML 1	1.19.0000 1.19.0000
My Web Se 1	
mZConfig 2	1.19.0000 9.03.0000
Nero Suite 1	
Netwaiting 1	2.5.59 2.5.59
NetWaiting 1	2.5.16 2.5.16
Network 2	140.0.215.140.0.215.000
NTRU TCG 1	2.1.36 2.1.36
NVIDIA Dri 3	
O2Micro Fl 1	3.0.07.23 3.0.07.23
O2Micro O 1	1.1.4.210C 1.1.4.210GS
O2Micro Sr 1	2.21.0000 2.21.0000
OCR Softw. 2	14.0 14.0
OGA Notifi 2	2.0.0048.0 2.0.0048.0

Oracle JInit 1	1.3.1.29	1.3.1.29
PC-CCID 1	2.0.0	2.0.0
PDF Compl 1	3.5.30	3.5.30
PhotoScap 1		
PhotoShow 1	2.0.063	2.0.063
PowerDVD 3	5.5	7.0
Preboot Ma 1	03.02.00.0	03.02.00.096
PrimoPDF - 3	4.1.0.11	5
Privacy Ma 1	1.0.0.528	1.0.0.528
Private Inft 1	07.00.00.0	07.00.00.047
ProductCor 3	50.0.165.0	140.0.000.000
QFolder 1	1.00.0000	1.00.0000
QlikView O 7	8.0.4783.1	8.0.4783.11
QuickSet 1	3.9.4	3.9.4
QuickTime 2	7.1	7.1
REALTEK G 1	1.00.0000	1.00.0000
Realtek Hiç 1		
RealUpgrac 1	1.1.0	1.1.0
Roxio Activ 3	1.0	1.0
Roxio Back 1	1.3.3	1.3.3
Roxio Burn 1	1.8	1.8
Roxio Crea 6	3.3.0	3.7.0
Roxio Crea 2	3.3.0	3.3.0
Roxio Crea 2	3.3.0	3.3.0
Roxio Crea 4	3.7.0	10.1
Roxio Crea 6	3.3.0	3.7.0
Roxio Crea 6	3.3.0	3.7.0
Roxio Crea 2	3.3.0	3.3.0
Roxio Crea 3	1.0.439	12.1.77.0
Roxio Crea 6	3.3.0	3.7.0
Roxio Drag 2	9.0	9.0
Roxio Expr 7	2.1.0	3.2.2
Roxio File l 1	1.3.2	1.3.2
Roxio MyD' 2	10.1.048	10.1.048
Roxio Upd 2	3.0.0	3.0.0
RS232ToU 1	3.6.1	3.6.1
Sage Advis 5	1.5.7.0	1.5.7.0
Sage Autol 3	1.0.1.0	1.0.1.0
Sage Fund 1	11.2.0.0	11.2.0.0
Sage Fund 6	11.2.0.0	11.2.0.0
Sage MIP F 4	9.0.0.0	10.1.0.0
Scan 2	140.0.167.	140.0.167.000
screensave 1		
Security U 11	KB228862:	KB960003
Security U 6	2.1.0.2	2.1.0.2
Security U 8	1	1
Security U 13	1	2
Security U 6	1	1
Security U 2	KB255309:	KB2553096

Spiceworks 1	5.3.75941	5.3.75941
SQLXML4 1	9.00.5000.	9.00.5000.00
Status 3	70.0.170.0	140.0.256.000
swMSM 1	12.0.0.1	12.0.0.1
Symantec , 1	10.1.5000.	10.1.5000.5
Symantec 1	12.0.1364	12.0.1364
Symantec 1	12.0.1364	12.0.1364
Symantec 1	2.0.0	2.0.0
Symantec 5	12.0.1364	12.0.1364
Symantec 16	11.0.5002.	11.0.5002.333
Symantec 1	11.0.5002.	11.0.5002.333
Symantec 1	5.0	5.0
Synaptics 2	11.0.7.0	15.0.17.4
SysAid Age 8	7.5	8.1
System Se. 1		
Tax Forms 7	6.5.5	11.3.13
Toolbox 5	1.00.0000	140.0.428.000
TrayApp 3	70.0.170.0	140.0.213.000
TreeSize Fr 1	V2.3.3	V2.3.3
Trusted Dri 1	4.1.1.312	4.1.1.312
UBitMenu 2	01.04	01.04
UGuide 2	1.00.0000	1.00.0000
Universal 1	4.2	4.2
Unlocker 1	1.8.9	1.8.9
Update for 3	KB967642	KB967642
Update for 8	1	1
Update for 6	1	1
Update for 3	1	1
Update for 3	KB255306!	KB2566458
Update for 1	KB253953(KB2539530
Update for 1		
Update for 2	KB952142	KB952142
Update for 1		
Update for 1		
Update for 2		
Update for 1		
Update for 1		
Update for 4	KB932080	KB934391
Upek Toucl 1	1.2.004	1.2.004
User Profile 1	1.6.30	1.6.30
VideoLAN \ 1	0.8.6d	0.8.6d
Vista Busin 2	6.0.6001	6.0.6002
Vista Defal 2	1.0.6.1	1.0.6.1
Waterfalls . 1		

Wave Infra 1	07.03.17.0	07.03.17.0010
Wave Supp 1	05.12.00.0	05.12.00.036
WebFldrs X8	9.50.7523	9.50.7523
WebReg 3	70.0.170.0	140.0.213.017
Windows 2 1	5.2.3790	5.2.3790
Windows 7 2	6.1.7600	6.1.7600
Windows 7 1	6.1.7601	6.1.7601
Windows C 1	3.0.04506.	3.0.04506.30
Windows D 1	05/13/200	05/13/2009 8.4.2.0
Windows D 1	09/11/200	09/11/2009 1.0.1.6
Windows D 1	12/27/200	12/27/2006 8.0.0.0
Windows F 19	1.3.3555.0	1.3.3555.0
Windows G 1	1.3.0254.0	1.3.0254.0
Windows G 3	1.7.0018.5	1.9.0040.0
Windows G 6	1.7.0036.0	1.7.0069.2
Windows Ii 6	3.0.0.0	3.0.0.0
Windows Ii 2	9.4.5000.0	9.4.5000.00
Windows Ii 19	6	9
Windows L 3	14.0.8064.	15.4.3502.0922
Windows L 5	14.0.8064.	15.4.3508.1109
Windows L 3	6.500.316!	7.250.4225.0
Windows L 2	15.4.3502.	15.4.3502.0922
Windows L 1	15.4.3502.	15.4.3502.0922
Windows L 1	15.4.3502.	15.4.3502.0922
Windows L 2	15.4.5722.	15.4.5722.2
Windows L 2	8.1.0178.0	15.4.3502.0922
Windows L 1	15.4.3502.	15.4.3502.0922
Windows L 2	15.4.3502.	15.4.3502.0922
Windows L 2	15.4.3502.	15.4.3502.0922
Windows L 3	14.0.8064.	15.4.3502.0922
Windows L 2	15.4.3502.	15.4.3508.1109
Windows L 1	15.4.5722.	15.4.5722.2
Windows L 1	15.4.5722.	15.4.5722.2
Windows L 1	15.4.5722.	15.4.5722.2
Windows L 1	15.4.5722.	15.4.5722.2
Windows L 1	5.000.818.	5.000.818.5
Windows L 2	15.4.3502.	15.4.3502.0922
Windows L 2	15.4.3502.	15.4.3502.0922
Windows L 2	14.0.8064.	14.0.8064.206
Windows L 1	14.0.8014.	14.0.8014.1029
Windows L 2	15.4.3502.	15.4.3502.0922
Windows L 2	15.4.3502.	15.4.3508.1109
Windows L 1	15.4.3502.	15.4.3502.0922
Windows L 1	15.4.3502.	15.4.3502.0922
Windows M 1		
Windows M 2		
Windows M 1	10	10
Windows M 2	11	11

Windows P 1	3.0.6920.0	3.0.6920.0
Windows S 5	5.2.3790	5.2.3790
Windows S 5	2	20070217.021455
Windows S 1	3.2.7600.2	3.2.7600.226
Windows S 1	2.5	2.5
Windows S 3	5.2.3790	5.2.3790.3959
Windows V 14		
Windows V 1	3.0.4203.2	3.0.4203.2
Windows X 8	5.1.2600	5.1.2600
Windows X 6	20080414.	20080414.031525
Wireless S 1	1.43.0.8	1.43.0.8
XML Paper 2	1.0	1.0
Yahoo! Det 1		
Yahoo! Toc 1		
Zebra P63C 1	3.02.02	3.02.02

Anejo P

Lydia Carrasquillo

From: William Velazquez Hiraldo
Sent: Thursday, September 13, 2012 3:15 PM
To: Lydia Carrasquillo
Subject: FW:

William Velázquez Hiraldo

Encargado de la Propiedad
Tel. (787) 721-4142
Fax (787) 727-0486
email: wvelazquez@rst.gobierno.pr



From: William Velazquez Hiraldo
Sent: Jueves, 13 de Septiembre de 2012 03:09 p.m.
To: Angel L. Diaz Marrero
Cc: Milagros Santiago
Subject:

SAGEFAS GOV

sage software

Version 2008.1
Copyright © 1994-2008
Sage Software, Inc.
All Rights Reserved

www.sagefas.com
800-368-2405

Registered to CST
Customer Number 0000041613084

Start | SageFAS_Engine | 03:07 p.m.

Anejo Q



COMISIÓN PARA LA
SEGURIDAD EN EL TRÁNSITO
GOBIERNO DE PUERTO RICO

COMISION PARA LA SEGURIDAD EN EL TRÁNSITO

Estrategia de Resguardo y Recuperación de Datos

Agosto 2012

Estrategia de Resguardo y
Recuperación de Datos