REGLAMENTO PARA EL USO ADECUADO Y LA SEGURIDAD DE LOS SISTEMAS DE INFORMÁTICA Y EQUIPOS TECNOLÓGICOS DE LA CORPORACIÓN DEL FONDO DEL SEGURO DEL ESTADO

Número: 9171

Fecha: 13 de marzo de 2020

***Aprobado*: Lcda. María Marcano de León**
Subsecretaria de Estado

Lcdo: Samuel Wiscovitch Coralí
Secretario Auxiliar de Servicios
Departamento de Estado
Gobierno de Puerto Rico

TABLA DE CONTENIDO

		Página
I.	Introducción	1 – 2
II.	Base Legal	2
III.	Propósito	2 – 3
IV.	Aplicabilidad	3
V.	Definiciones	3 - 9
VI.	Disposiciones	9
	A. Titularidad y Derechos	9 – 10
	B. Responsabilidades de la Oficina de Sistema de Información	10 – 15
	C. Uso y Manejo de Recursos Informática	15 – 20
VII.	Política de Seguridad	20
	A. Responsabilidad, Manejo y Disposición de los Equipos	20
	B. Almacenamiento e Intercambio de Archivos	21
	C. Programas y Aplicaciones de la CFSE	22
	D. Licencias	22
	E. Utilización de Correo Electrónico, Internet y Mensajería Instantánea	23 – 26
	F. Acceso y Solicitud de Acceso	26 – 27
	G. Utilización de Contraseñas	28 – 29
	H. Tecnologías en la Nube (Cloud Computing)	29 – 31
	I. Conexión Remota	32
	J. Aplicaciones de Servicios	32 – 33
	K. Disposiciones de Equipos e Información	33 – 34
	L. Cuentas Inactivas	34

M. Protección y Cuidado de Equipos de Periferales 34 – 35

N. Manejo y Documentación de Incidentes, Problemas y Peticiones 35

O. Política sobre el Servidor de Seguridad de Computadoras y Redes 35 – 36

P. Monitoreo de los Sistemas Tecnológicos y Pruebas de Control y Vulnerabilidad 36 – 39

Q. Programa de Continuidad 40

R. Control Ambiental de los Recursos de Informática 41

S. Boletín Informativo de Medidas de Seguridad 41

T. Cumplimiento de Política 41 – 42

VIII. Salvedad 42

IX. Derogación 42

X. Aprobación 43

XI. Vigencia 43

REGLAMENTO PARA EL USO ADECUADO Y LA SEGURIDAD DE LOS SISTEMAS DE INFORMÁTICA Y EQUIPOS TECNOLÓGICOS DE LA CORPORACIÓN DEL FONDO DEL SEGURO DEL ESTADO

ARTÍCULO I – INTRODUCCIÓN

La Corporación del Fondo del Seguro del Estado (CFSE) ofrece una variedad de servicios a diversos sectores y cumple una serie de funciones sociales muy importantes a favor del pueblo de Puerto Rico. Por la complejidad de sus operaciones, la CFSE ha invertido significativamente en sus recursos de tecnología y en la actualización de sus sistemas de información, lo que ha resultado en beneficio de nuestros lesionados, patronos, empleados, y público en general. Consecuentemente, la CFSE ha asumido un firme compromiso de velar por el uso responsable de sus equipos y de proteger sus datos confidenciales, restringidos y sensitivos, para evitar su uso inapropiado y mantener sus equipos, sistemas de información, comunicaciones y conexiones seguras y libres de obstáculos.

Los aparatos electrónicos propiedad de la CFSE son utilizados por los empleados, contratistas y afiliados para mantener de manera óptima las operaciones de la CFSE. Estos aparatos electrónicos contienen información sensitiva de la CFSE y se conectan a los sistemas de información. Por ello, deben estar protegidos de su mal uso para garantizar la seguridad, disponibilidad, y confianza en los sistemas de información de la CFSE. El mal uso de estos servicios puede comprometer la integridad, seguridad, confidencialidad y el acceso a información vital, lo que puede causar daños a la CFSE.

Este Reglamento identifica las responsabilidades de los empleados y contratistas de la CFSE, de los usuarios de los sistemas de información de la CFSE y de la OSI y su Director, relacionados al uso aceptable de los equipos, recursos y redes de comunicaciones y computación, y para el acceso a información confidencial de la CFSE. Del mismo modo, este Reglamento establece los mecanismos, guías, parámetros y normas para garantizar la integridad, confidencialidad y disponibilidad de la información que la CFSE maneja para los patronos, lesionados, empleados y operaciones de sus distintas dependencias.

ARTÍCULO II – BASE LEGAL

Este Reglamento se adopta de conformidad con los poderes conferidos a la Junta de Gobierno y al Administrador de la CFSE mediante los Artículos 1B-3 y 1B-4 de la Ley Núm. 45 de 18 de abril de 1935, según enmendada, conocida como la "Ley del Sistema de Compensaciones por Accidentes del Trabajo"; y la Ley Núm. 38 de 30 de junio de 2017, según enmendada, conocida como la "Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico", y la Carta Circular Núm. 140-16 del 7 de noviembre de 2016, de la Oficina de Gerencia y Presupuesto, conocida como "Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales".

ARTÍCULO III – PROPÓSITO

El propósito de este Reglamento es establecer los mecanismos, guías, parámetros y normas para garantizar el uso adecuado y responsable de los equipos y sistemas tecnológicos. Además, establece los controles para el uso adecuado de la información que se maneja a través de los sistemas electrónicos. Provee las herramientas de monitoreo para el acceso a Internet, Intranet y correo electrónico para garantizar la integridad y la disponibilidad de la información que se maneja. Establece los mecanismos para disponer del equipo

de tecnología de información y de los programas instalados, el mantenimiento del equipo, así como la confiabilidad y manejo de los datos bajo la custodia de la CFSE en sus sistemas de información.

ARTÍCULO IV – APLICABILIDAD

Las disposiciones de este Reglamento serán de aplicabilidad a todo funcionario de la CFSE, sea de confianza, gerencial, o unionado, con carácter regular, transitorio o temporal, así como a todo contratista, consultor y cualquier persona relacionada a la CFSE que sea custodio o utilice algún equipo tecnológico o acceda a la red de comunicaciones de la CFSE.

ARTÍCULO V – DEFINICIONES

Para propósito de este Reglamento, los términos que se mencionan a continuación se interpretarán, según la definición que le acompaña.

A. Administrador: Administrador de la CFSE.

B. Adware: Programa que se instala inadvertidamente en una computadora y que su principal propósito es desplegar anuncios y propaganda, pero también puede tener un comportamiento como spyware.

C. Análisis de Riesgos: Informe gerencial que determina la probabilidad y el impacto de una variedad de amenazas específicas que puedan causar interrupción de negocios.

D. Análisis de Impacto: Informe gerencial donde se determina la prioridad en los procesos críticos de los negocios sus impactos cualitativos y cuantitativos, los costos por interrupciones, y el tiempo de recuperación necesario de los procesos críticos.

E. Antivirus: Programa que protege a los sistemas de información de los ataques de virus conocidos.

F. Aprovisionamiento: Preparar y acondicionar un sistema o aplicación para un usuario o grupo de usuarios.

G. Oficina de Sistemas de Información (OSI): Unidad operacional adscrita al Administrador de la CFSE cuya función es realizar labores esenciales y procurar el óptimo funcionamiento de los sistemas de información.

H. Autenticación: Proceso por el cual una persona presenta información que lo identifica ante un sistema de información, donde el sistema corrobora la información entrada con la información en su base de datos para validarla.

I. Autorización: Proceso por el cual se adjudican privilegios específicos a una persona para el uso de recursos en los sistemas de información.

J. Cifrar o cifrado (Encrypt): Proceso a través del cual se transforman datos a un formato que no puede traducirse fácilmente por personas no autorizadas a acceder los mismos.

K. Cloud Computing (Tecnologías en la nube): Modelo para habilitar de forma conveniente, ubicua y por demanda (según sea solicitado) el acceso en red a un conjunto de recursos informáticos compartidos y confiables que puedan ser prestados de forma rápida y lanzados con un mínimo de esfuerzo de gestión o interacción de parte del proveedor del servicio.

L. CFSE: Corporación del Fondo del Seguro del Estado.

M. Contraseña (Password): Secuencia de caracteres que se utiliza para proveer acceso a una persona particular, con el fin de comprobar que el usuario que está requiriendo acceso a un sistema es realmente ese usuario.

N. Correo electrónico: Servicio de transmisión de mensajes a través de una red.

O. Disco Duro: Dispositivo encargado de almacenar archivos e información de forma permanente y reutilizable en una computadora.

P. Disposición de Equipo: Proceso de eliminar equipo perteneciente a la agencia y destruir el equipo determinado obsoleto, inservible, o para el cual haya culminado su vida útil.

Q. Empleado: Funcionario que laboran en la CFSE.

R. Equipo Computadorizado: Dispositivo o máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil. Se

compone físicamente por numerosos circuitos integrados y otros muchos componentes de apoyo, extensión y accesorios, que en conjunto pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa. Dos partes esenciales constituyen estos equipos: el hardware, que es su componente físico (circuitos electrónicos, cables, gabinete, teclado, entre otros) y el software, que consta de la parte intangible (sistemas operativos, programas, datos, información, entre otros) del equipo. Hardware y software trabajan en conjunto para operar el equipo computadorizado.

S. Files Exchange System (FEX): Herramienta o aplicación para el intercambio de documentos de la CFSE con personal interno y entidades o personas externas.

T. Fraude Cibernético: Uso de la computadora, del internet, de los correos electrónicos, o cualesquiera medios informáticos, y mediante cualquier manipulación informática, se defraude o se consiga la transferencia no consentida de datos, información, documentos o cualquier bien o derecho patrimonial en perjuicio de un tercero, o de la Corporación del Fondo del Seguro del Estado, o del Gobierno de Puerto Rico. Entre las formas de fraude cibernético están la piratería informática (hacking) y la intercepción de una transmisión electrónica, entre otros.

U. HIPAA (Health Insurance Portability and Accountability Act, Pub. L. No. 104-101, 110 Stat. 1936 1996): Ley que establece los estándares para la protección de la información de salud individualmente identificable, los estándares nacionales para la seguridad electrónica de la información de salud protegida; la Regla de Notificación de Violación de Seguridad, la cual requiere que las entidades y los asociados de negocio cubiertos a proveer una notificación luego de una violación de seguridad de la información de salud protegida y las disposiciones sobre confidencialidad de la Regla de Seguridad del Paciente, la cual protege la información de identidad utilizada para analizar los eventos de seguridad del paciente y mejorar la seguridad del paciente.

V. Internet: Red mundial que permite el intercambio de información y acceso a servicios, tales como páginas de portales, correo electrónico, entre otros.

W. Intranet: Red interna de la CFSE que se accede desde varias localizaciones y utiliza los mismos protocolos de comunicación que la internet.

X. Lenguaje discriminatorio: Expresiones que podrían percibirse como ofensivas o discriminatorias, ya sea por razones de edad, raza, color, sexo, orientación sexual, identidad de género, origen social o nacional, condición social, afiliación política, ideas políticas o religiosas, por ser víctima o ser percibida como víctima de violencia doméstica, agresión sexual, o acecho, por ser militar, ex militar, servir o haber servido en las Fuerzas Armadas de los Estados Unidos o por ostentar la condición de veterano.

Y. Licencia para programas (software): Contrato entre el autor del programa y el usuario, que le permite al usuario utilizar el programa de forma legal.

Z. Malware: Programa diseñado para infiltrar y dañar un sistema de computadoras sin el consentimiento informado de su dueño. Es un término general que se refiere a cualquiera de las formas que puede tomar un programa o código hostil, intrusivo y/o molestoso a un sistema de computadoras.

AA. Monitoreo: Sistema de control, supervisión, filtro o control de una red de ordenadores para detectar defectos, irregularidades, correos electrónicos no solicitados (spam), actividades sospechosas o no relacionadas con las operaciones o los trabajos de la Corporación del Fondo del Seguro del Estado, o problemas en la red. Incluye además, el control sobre el equipo (servidores, computadoras, computadoras portátiles, tabletas, y equipo de comunicación, entre otros), y los programas que permiten el almacenamiento, el recibo, la transmisión y el procesamiento de la información de la Corporación del Fondo del Seguro del Estado.

BB. Nombre de usuario (Username): Secuencia de caracteres de conocimiento del usuario que éste utiliza para acceder a los sistemas de

información de la Corporación del Fondo del Seguro del Estado, y que se hace público a otros usuarios, o páginas cibernéticas, para recibir o proveer información, o para uso de identificación.

CC. Oficinas: Localidades de la CFSE que tienen acceso al sistema de información computarizado.

DD. Plan de Continuidad Gubernamental: La planificación y preparación con tiempo necesario para minimizar pérdidas y asegurar la continuidad de las funciones críticas de una organización ante la eventualidad de un desastre o contingencia.

EE. Plan de Recuperación de Desastres: Tareas, actividades y procedimientos formales conducentes al restablecimiento de los sistemas críticos de procesamiento ante la eventualidad de un desastre o contingencia.

FF. Periferales: Equipos electrónicos, tales como terminales, impresoras, computadoras, teclados, módems, enrutadores o "routers", interruptores o "switchs", entre otros.

GG. Remoción de Contenido: Proceso que elimina el contenido de los medios para almacenamiento de datos (discos duros, cintas magnéticas, memorias y otros), de tal manera que dicho contenido no pueda recuperarse de ese equipo en un futuro a través de diferentes métodos.

HH. Resguardo: Copia de información en los sistemas de informática.

II. Servicio Web (Web Service): Tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet. La interoperabilidad se consigue mediante la adopción de estándares abiertos.

JJ. Servidor de Seguridad de Computadoras y Redes (Firewall): Aplicación, equipo, o conjunto de ambos que protege los recursos en una red de accesos no autorizados.

KK. Seguridad de Informática o Cibernética (Cybersecurity): Protección de los sistemas de información en contra del acceso o modificación física o electrónica de la información. Protección en contra de la negación de servicios a usuarios autorizados o de la disponibilidad de servicios a usuarios no autorizados. Establece las políticas, normas, medidas, proceso y herramientas necesarias para detectar, documentar, prevenir y contrarrestar los ataques a la información o servicios antes descritos. Maneja procesos y herramientas necesarias para la restauración de la información o los sistemas afectados por las brechas en la seguridad; disponibilidad y protección de los recursos requeridos para establecer dicha seguridad.

LL. Sistema de Detección y Prevención de Intrusos: Es un programa que reside en una computadora o en un equipo especializado y que permite detectar ataques o intentos indebidos de acceso hacia un sistema de información.

MM. Sistemas de información: Se refiere a los equipos electrónicos computadorizados que se utilizan como herramienta de trabajo de la CFSE para uso y manejo de la información.

NN. Spyware: Programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización del internet.

OO. Universal Serial Bus (USB): Es un tipo de dispositivo de conexión que se usa comúnmente para almacenamiento de datos que utiliza memoria instantánea (flash) para guardar datos e información.

PP. Usuarios: Todos los empleados, contratistas independientes, consultores, patronos, lesionados, y cualquier otra persona o entidad que utilice la red de computadoras de la CFSE.

QQ. Virus: Programa de computadora cuyo fin es hacerle daño a la computadora donde reside.

RR. Virtual Private Network (VPN): Red tecnológica que se usa para conectar de remoto una o más computadoras a una red privada utilizando el Internet.

ARTÍCULO VI – DISPOSICIONES

A. Titularidad y Derechos

1. Los periferales, programas, documentos y servicios asociados al sistema de información son propiedad de la CFSE y solo podrán ser utilizados para propósitos lícitos, prudentes, responsables y que estén dentro de las funciones inherentes del puesto que ocupa cada empleado.
2. Todo equipo ejecutable que haya sido creado, adquirido, creado, desarrollado o modificado mediante el uso de cualquier recurso de informática adscrito o propiedad de la CFSE se considerara propiedad de la CFSE.
3. 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 las computadoras o el equipo tecnológico de la CFSE será propiedad de la CFSE, 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.
4. La información contenida en los equipos, computadoras, servicios asociados internos y externos, los mensajes de correo electrónico, Internet, Intranet, documentos o programas existentes no podrán ser reproducidos o utilizados para fines ajenos a las funciones y facultades de la CFSE; esta información estará disponible en todo momento para ser examinada o utilizada por el Administrador o su representante autorizado.

5. La información contenida en los equipos, computadoras, servicios asociados internos y externos, los mensajes de correo electrónico, Internet, Intranet, documentos o programas existentes es propiedad del Gobierno de Puerto Rico, y como tal le aplican todas las disposiciones aplicables a los documentos públicos, por lo que su divulgación, destrucción, alteración, fraudulenta o su uso para propósitos personales o privados puede constituir un delito.

B. Responsabilidades de la Oficina de Sistemas de Información

La Oficina de Sistemas de Información, (en adelante, "OSI") es responsable de:

1. Diseñar, implementar, mantener y realizar toda la seguridad en cuanto a sus redes, equipo (hardware), programación (software), datos y usuarios.
2. Establecer los controles necesarios para evitar que de forma intencionada o accidental se inicien ataques desde las redes y sistemas de la CFSE hacia sistemas de información externos.
3. Planificar los servicios internos y los métodos de apoyo a los usuarios de sus sistemas de información y equipos.
4. Configurar las computadoras y equipos de los usuarios de los sistemas de información.
5. Proveer apoyo a los usuarios de los sistemas de información de la CFSE.
6. Planificar y realizar el mantenimiento de sus sistemas internos.
7. Realizar auditorías de seguridad y verificar los equipos y sistemas de información regularmente para identificar averías, fallas, problemas y posibles modificaciones a los mismos para garantizar que se mantengan en un nivel de calidad óptima y a su vez obtener los datos relevantes sobre las necesidades en los sistemas de información para la confección del presupuesto de la CFSE.
8. Obtener la aprobación de Área de Tecnología de Información de la Oficina de Gerencia y Presupuesto del Gobierno de Puerto Rico

(ATI) sobre proyectos de tecnología y sistemas de información previo a su contratación por parte de la CFSE.

9. Notificar a ATI sobre cualquier evento crítico que genere alto volumen de uso de las redes y sistemas de la CFSE para que ATI colabore para asegurar la disponibilidad y continuidad del servicio, de entenderlo necesario.
10. Notificar a ATI sobre cualquier proyecto relacionado a tecnologías de la información a través de la aplicación LEAN-Tech o en el sistema en uso al momento para los mismos efectos.
11. Generar peticiones de servicio a la División de Asistencia Técnica de ATI cuando lo estime necesario.
12. Comunicar a los usuarios de los sistemas de información de la CFSE todos los asuntos relacionados a las políticas, protocolos, guías, reglamentos o manuales sobre los sistemas de información que le apliquen.
13. Comunicar a los empleados y contratistas de la CFSE los procedimientos para responder a distintos tipos de incidentes que pongan en riesgo, directa o indirectamente las redes, sistemas de información y equipos de la CFSE.
14. Hacer y presentar a la ATI un análisis de Costo Total de Administración en el cual se evalúe los costos de adquisición, implementación, educación y manejo de cambios administración, mantenimiento, política de manejo de parchos/upgrades, plan de continuidad de negocios y recuperación de desastres.
15. Asegurar que la CFSE adquiera el licenciamiento necesario para el uso de programas, aplicaciones y periferales, y realizar las recomendaciones correspondientes para la adquisición de todo el equipo y de todas las plataformas y licencias necesarias para el funcionamiento de su red interna y que las licencias se registren a nombre de la CFSE con las empresas que posean los derechos propietarios sobre las mismas.

16. Mantener actualizado el inventario de las licencias bajo la propiedad de la CFSE que no están en uso o que están disponibles para ello y disponer las licencias que no están en uso o no están autorizadas para su uso.
17. Establecer controles de autenticación, autorización, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información.
18. Implementar y utilizar mecanismos de autenticación y autorización de usuarios, tales como el método de asignación de un nombre de usuario (username) y contraseña (password) particular para cada usuario para garantizar el uso adecuado, efectivo y seguro del Internet y del correo electrónico.
19. Asegurar la continuidad de sus operaciones mediante un Plan de Recuperación por Desastre para asegurar la programación (software), el equipo (hardware), datos y facilidades físicas de la CFSE.
20. Mantener una copia de todas las políticas, protocolos, guías, reglamentos o manuales sobre los sistemas de información accesibles a los usuarios de los sistemas de información y equipos de la CFSE.
21. Bloquear el acceso a páginas y todo tipo de contenido pornográfico.
22. Verificar que el sitio web cuenta con todos los mecanismos en vigor para protección adecuada para la información de la CFSE.
23. Establecer mecanismos, equipos, programas, y sistemas para detectar, prever, y reportar accesos no autorizados a sus redes, sistemas de información y equipos, de modo que garanticen la confidencialidad de la información de accesos no autorizados utilizando el firewall como uno de los mecanismos de seguridad.
24. Verificar que el intranet, internet y el correo electrónico estén funcionando adecuadamente.

25. Resguardar (back-up) los datos y sistemas de acuerdo a la política de retención aplicable a cada sistema.
26. Administrar el acceso de los usuarios a los sistemas de información y equipos de la CFSE, incluyendo, pero sin limitarse al acceso a servidores, cuentas de acceso, impresoras, y acceso a equipo y programación especializada.
27. Establecer los controles necesarios para asegurar que aquellos equipos que hayan estado fuera de la CFSE no representen un riesgo a sus redes y sistemas de información mediante la revisión, auditoría y monitoreo de dichos equipos previo y luego de a ingresarlos al sistema.
28. Documentar la información de los usuarios que acceden a sus sistemas en una base de datos, donde consten los nombres de las personas con accesos y el tipo de acceso aprobado.
29. Establecer procesos que permitan monitorear las actividades de los usuarios en el uso de, o acceso a aquellos activos sensitivos que lo ameriten.
30. Establecer e instalar controles automáticos para la prevención y detección de programas no deseados, tales como virus, spyware, malware, adware, y actualizaciones automáticas.
31. Administrar y actualizar los sistemas de información para la protección contra antivirus, antimalware y firewalls.
32. Disponer adecuadamente del equipo obsoleto, cuya vida útil haya culminado, averiado o en desuso, y asegurar que previo a ello, dicho equipo no contenga programación o información sensitiva y/o confidencial mediante un proceso de eliminación de programas e información.
33. Colocar un aviso para las personas que accedan los sistemas de información de la CFSE notificándoles que están entrando en un sistema de información propiedad del Gobierno de Puerto Rico por lo que deben conocer y cumplir con las normas aplicables.

34. Realizar una evaluación de riesgos, según la Orden Administrativa de Análisis de Riesgo vigente.
35. Probar y avalar el desarrollo de soluciones o los requisitos de seguridad de un programa o aplicación implementada en la CFSE a través de la metodología de desarrollo, operación, mantenimiento de programas o aplicaciones utilizado por la CFSE, conocida como Software Development Life Cycle.
36. Definir y actualizar periódicamente los estándares de conexión a la red desde cualquier punto para minimizar la exposición a posibles daños, incluyendo conexiones de dial-up, virtual private network (VPN), o cualquier otra tecnología útil para este propósito.
37. Establecer políticas, procedimientos, guías, normas o protocolos sobre:
    a. Plan de Recuperación por Desastre para asegurar la programación (software), el equipo (hardware), datos y facilidades físicas de la CFSE.
    b. Procesos para monitorear actividades en activos sensitivos.
    c. Procedimientos para detectar, reportar, y responder a incidentes de seguridad que incluyan límites de tiempo máximo y mínimo para la respuesta a distintos tipos de incidentes.
    d. Procedimientos que permitan realizar y documentar los cambios a la seguridad de los sistemas y a su vez asegure dicha documentación.
    e. Mecanismos para mantener a los empleados de la OSI adiestrados, capacitados y actualizados respecto a los aspectos de seguridad pertinentes a la CFSE y sus respectivas áreas.
    f. Mecanismos para capacitar a todos los empleados y usuarios sobre los controles de seguridad, los usos y seguridad de los sistemas de información de la CFSE periódicamente.
    g. Políticas sobre el uso adecuado, efectivo y seguro del internet y del correo electrónico, aplicables a todos los usuarios de los

sistemas de información de la CFSE, que indique los usos permitidos y no permitidos del internet, las sanciones y medidas disciplinarias que podrían aplicar a los usuarios que incumplan con ellas. Esta política deberá ser entregada a cada usuario, quien firmará acertando que conoce la política y que cumplirá con esta.

h. Normas sobre la asignación de cuentas de acceso.

i. Normas sobre el uso de cifrado en comunicación de información sensitiva o confidencial a través del correo electrónico.

j. Análisis de riesgos

k. Análisis de impacto

l. Protocolo de Resguardo

m. Plan de Continuidad Gubernamental

C. Uso y Manejo de Recursos de Informática

En general:

1. Ningún empleado y/o contratista de la CFSE utilizará los sistemas de información de la CFSE, incluyendo las computadoras personales o portátiles, para propósitos personales, de recreo, manejo de negocio propio o asuntos privados del usuario.
2. Se prohíbe el almacenamiento de archivos, data, programas o aplicaciones para propósitos personales o manejo de negocios o transacciones personales o para cualquier otro asunto o servicio no oficial o ajeno a las funciones de la CFSE.
3. Ningún empleado de la CFSE utilizará los sistemas de información de la CFSE, incluyendo las computadoras personales o portátiles, para bajar (download) películas ni programas pirateados del internet ni de ningún sistema.
4. Para asegurar que la información de la CFSE se mantenga segura, confidencial y disponible, al utilizar cualquier equipo, o al acceder a

cualquier plataforma o medio para reproducir información de la CFSE, todo usuario debe:

a. Mantener secreta toda información de acceso a cualquier cuenta relacionada a la CFSE, y no compartir dicha información con individuo alguno, ni a personal de servicio técnico de la CFSE.
b. Evitar utilizar las mismas claves y contraseñas que utiliza para acceder información y cuentas de la CFSE para acceder a información o cuentas privadas o de entidades ajenas a la CFSE.
c. Mantener cubiertas y cerradas las pantallas de los aparatos electrónicos de modo que nadie pueda accederlas sin aprobación o conocimiento cuando no estén en uso.
d. Cerrar la sesión luego de cada uso y asegurar que el aparato físico está debidamente almacenado y protegido cuando esté desatendido por largos periodos de tiempo.
e. Desconectar el dispositivo o escritorio virtual de cualquier conexión a acceso remoto cuando ya no esté utilizando dicha conexión activamente.
f. Remover y asegurar cualquier dispositivo de almacenaje o de uso que contenga cualquier información de la CFSE, cuando dicho dispositivo no esté siendo utilizado activamente.
g. Reportar cualquier pérdida, hurto o robo a su equipo, dispositivo de almacenaje o accesorio que contenga o pueda contener información de la CFSE, inmediatamente y nunca luego de 24 horas de haber conocido del suceso, según el Reglamento Interno para el Uso, Control, y Contabilidad de la Propiedad Mueble de la Corporación del Fondo del Seguro del Estado, vigente.

h. Cumplir a cabalidad con todos los requisitos establecidos para políticas de seguridad sobre el acceso y manejo de información, así como para el manejo de emergencias.

i. Acceder y utilizar aplicaciones y programas aprobados, descargados e instalados por la OSI, o las autoridades pertinentes en la CFSE.

j. Devolver a la CFSE todo equipo, dispositivo, y activos en su posesión al terminar su empleo, contrato o acuerdo con la CFSE, según el Reglamento Interno para el Uso, Control, y Contabilidad de la Propiedad Mueble de la Corporación del Fondo del Seguro del Estado, vigente.

k. Asegurar que los dispositivos de almacenaje portátil estén custodiados dentro de las facilidades de la CFSE, de necesitar alguna copia de seguridad del contenido de su equipo o dispositivo de la CFSE si la información que contiene es altamente sensitiva, el dispositivo deberá contar con un cifrado aprobado para proteger su contenido.

l. Cumplir con todas las disposiciones y reglamentaciones provistas para las patentes, marcas, derechos de autor de cada programa o material evaluado, observado, utilizado u obtenido mediante el internet.

m. Respetar la privacidad y reputación de otros individuos y organizaciones cuando se comunique información a través del internet.

n. Asegurar que la información confidencial y sensitiva de la CFSE sólo sea divulgada y/o publicada siempre y cuando sea aprobada por la Oficina de Sistemas de Información.

o. No utilizar servicios o sitios que se acceden a través del internet para procesar o almacenar información de la CFSE sin contar con la aprobación de las debidas autoridades dentro de la CFSE.

p. Reportar inmediatamente cualquier asunto de seguridad, identificado o sospechado a su supervisor inmediato y a las debidas autoridades dentro de la CFSE.

5. Está prohibido el uso de la red de computadoras, equipo, los programas y las aplicaciones de los sistemas de información de la CFSE, durante horas laborables, tiempos de recesos y periodos de tomar alimentos (periodos de almuerzo) para:

a. Difundir, acceder, almacenar crear, transmitir, o enviar información ilegal, fraudulenta, amenazante, sexualmente explícita, obscena, intimidante, irreverente o difamatoria, o material inapropiado u ofensivo, tales como comentarios sobre raza, sexo o género, características físicas, discapacidades, edad, orientación sexual, u origen nacional, creencias o prácticas religiosas o políticas, o pornografía.

b. El envío de correo que no sea oficial, así como el envío de material ofensivo, fraudulento, amenazante, ilegal, difamatorio, pornográfico, o de cualquier otra índole no autorizada.

c. Descargar (download) películas, programas o cualquier tipo de aplicación hurtada o que sea producto de la piratería, aunque sean libres de costo.

d. Acceder la información o a una cuenta ajena sin autorización que se obtiene mediante la modificación de privilegios de acceso o la interceptación de información.

e. Reproducir maliciosa o voluntariamente de un virus.

f. Realizar actividades que estén en contra de la Ley de Ética Gubernamental (Ley 1 de 2012).

g. Promover actividades no relacionadas al CFSE, o que sean para beneficio personal.

h. Realizar actividades que puedan afectar o potencialmente afectar la reputación de la CFSE, el Gobierno de Puerto Rico, y sus funcionarios y empleados.

i. Recibir y enviar mensajes en cadena.

j. Acceder sitios web o aplicaciones de compras, juegos, concursos, encuestas, o páginas de entretenimiento.

k. Difundir material y/o el acceso a material político partidista.

l. Proveer información confidencial de la CFSE a ninguna persona, individuos u organizaciones que no tengan autorización ni necesidad de conocer esta información.

m. Interferir con las operaciones internas o externas de la CFSE.

n. Intentar ganar acceso a información, redes, aplicaciones o páginas web a las que no tenga autorización acceder.

o. Registrar las redes y sistemas para hallar información personal de otros individuos, incluyendo archivos de personal, archivos personales e información sobre claves y contraseñas de acceso sin la debida autorización.

p. Engañar a otros o a la CFSE en cuanto a su posición, autorización, o capacidades.

q. Promover comportamiento antiético o antisocial.

r. Realizar actividades que violen leyes o regulaciones internacionales, estatales, federales, o locales.

s. Realizar actividades inconsistentes con la visión, misión, objetivos y/o valores del Gobierno de Puerto Rico y la CFSE.

t. Abrir algún programa que, aún con la debida autorización para ello, se sospeche pueda contener malware.

u. Modificar la configuración del internet de modo que pueda burlar las políticas y requisitos de seguridad de la CFSE.

v. Descargar material protegido bajo las leyes de derechos de autor del internet sin aprobación de sus supervisores o jefes de la agencia, o personal de la OSI.

w. Acceder información privada y otro material no-público en el internet sin obtener la aprobación apropiada del propietario de la información o material.

x. Participar de juegos recreacionales no relacionados a sus funciones laborales en la CFSE.

y. Realizar actos que violenten las protecciones a patentes, derechos de autor, derechos de marca o derechos de propiedad intelectual.

z. Cualquier uso ajeno a las funciones del CFSE y del empleado, o no autorizado expresamente.

ARTÍCULO VII – POLÍTICA DE SEGURIDAD

A. Responsabilidad, Manejo y Disposición de los Equipos

1. Los empleados o personas custodias de la propiedad a quienes se les asigne cualquier equipo tecnológico, incluyendo computadoras personales o portátiles, serán responsables de custodiar el mismo y mantenerlo en un lugar seguro y libre de riesgos que puedan afectar su funcionamiento.
2. Todo equipo o periferal en posesión de cualquier empleado que luego de ser evaluado sea puesto en desuso, deberá ser decomisado, según el Reglamento Interno para el Uso, Control, y Contabilidad de la Propiedad Mueble de la Corporación del Fondo del Seguro del Estado, vigente.
3. Está prohibida la transferencia, donación, o retención de equipo tecnológico de la CFSE luego que sea puesta en desuso, declarado excedente, inservible u obsoleta, y no haya sido decomisada según dispone el Reglamento Interno de Propiedad de la CFSE, vigente.
4. Todo usuario custodio deberá devolver a la CFSE todo equipo, dispositivo, y activos en su posesión al terminar su empleo, destaque, licencias, contrato o acuerdo con la CFSE, o una vez culmine el proyecto, tarea, o situación por la cual dicho equipo, dispositivo o activo estuvo en su posesión, según dispone el Reglamento Interno de Propiedad de la CFSE, vigente.

B. Almacenamiento e Intercambio de Archivos

1. Solo se podrá utilizar dispositivos USB para almacenamiento de datos cuando exista previa autorización escrita por parte del Director de Sistemas de Información, y previo a la entrega y aprobación del formulario CFSE 12-001, Solicitud para la Creación, Cancelación o Sustitución de Contraseñas para el Uso de USB y VPN completo en todas sus partes.
2. Todo intercambio de archivos con entidades externas con información financiera, de salud, confidencial o protegida deberán utilizar la aplicación FEX.
3. Los usuarios de equipos de almacenamiento e intercambio de archivos dentro de la CFSE deberán observar las siguientes normas:
   a. No modificar las configuraciones de seguridad o las configuraciones anti-malware de su dispositivo o escritorio virtual para su labor con la CFSE, ni cualquier configuración que pueda tener el efecto de evitar los requisitos que establece esta política.
   b. No participar de juegos recreacionales, no relacionados a la CFSE.
   c. No realizar actos que violenten las protecciones a patentes, derechos de autor, derechos de marca o derechos de propiedad intelectual.
   d. El uso de dispositivos personales para dentro de las redes y sistemas de información de la CFSE debe ser evaluado y aprobado por el Director de la OSI para asegurar que no sea un riesgo de seguridad.
   e. Asegurar que su dispositivo cuente con los requisitos de seguridad necesarios para acceder aplicaciones de la CFSE cuando estas están disponibles y permiten el acceso.

f. No conectar dispositivos de almacenaje personales ni que provengan de fuentes no confiables en los equipos y dispositivos de la CFSE.

C. Programas y Aplicaciones de la CFSE

1. La seguridad de la información deberá ser parte integral del diseño de cualquier programa de aplicación que adquiera o desarrolle la CFSE para facilitar sus operaciones o los servicios que provee.
2. Ningún empleado podrá descargar y/o instalar programas o aplicaciones en los equipos, computadoras y sistemas de informática de la CFSE, que no hayan sido adquiridos por ésta, aun cuando sean gratis, excepto mediante autorización escrita del Director de la OSI.
3. Está prohibido copiar programas o aplicaciones de computadoras adquiridas por la CFSE.
4. Se prohíbe el acceso a o la utilización de propiedad intelectual (copyright information) cuando tal acceso o utilización viole derechos de autor.
5. Se prohíbe el uso de los sistemas de información de la CFSE, incluyendo el correo electrónico, para el envío o la divulgación a personas no autorizadas de información financiera, confidencial o de información protegida al amparo de la HIPPA o de cualquier otra Ley o Reglamento vigente.

D. Licencias

1. La OSI se asegurará de que la CFSE adquiera el licenciamiento necesario para el uso de programas, aplicaciones y periferales.
2. La OSI se asegurará de que las licencias se registren a nombre de la CFSE con las empresas que posean los derechos propietarios sobre las mismas.
3. Se prohíbe el uso de programas, aplicaciones, o equipos para los cuales no exista una licencia o autorización de uso válida a nombre de la CFSE.

E. Utilización del Correo Electrónico, Internet y Mensajería Instantánea

1. Los correos electrónicos y envío de mensajes instantáneos son canales electrónicos internos vitales para la comunicación dentro de la CFSE, por lo que estos solo serán utilizados para fines oficiales y legales por personal debidamente autorizado.
2. La comunicación a través del Internet desde el CFSE estará controlada por un firewall para proteger el sistema contra accesos no autorizados.
3. La OSI proveerá accesos al correo electrónico y al internet a aquellos empleados cuyas funciones en la CFSE así lo requieran.
4. El uso de contraseñas (password) u otro método para autenticación y autorización de usuarios para tener acceso al correo electrónico y al internet desde los equipos de la CFSE no será obstáculo para que se realicen auditorías al sistema cuando sea necesario y requerido.
5. La OSI tendrá acceso en cualquier momento a los mensajes electrónicos e información de los espacios virtuales (web) visitados por los usuarios para auditoria o investigación cuando sea necesario o requerido, y los mismos serán considerados parte de los expedientes y documentos oficiales de la CFSE.
6. La OSI restringirá el envío de correos electrónicos de aquellas fuentes que sean categorizadas como correo no deseado (spam) o virus o de códigos maliciosos; así como accesos a páginas de internet y redes sociales, con la excepción de aquellos casos en que exista una debida justificación y medie autorización de acceso por parte del Administrador.
7. El usuario no alberga expectativa de intimidad alguna con relación a la información, los documentos y/o mensajes creados, recibidos o enviados a través del sistema de correo electrónico o el servicio

de internet de la CFSE, independientemente sean remitidos a través desde cuentas personales.

8. El propósito primordial del uso de servicios de email y mensajería instantánea es mantener el desempeño de la CFSE en sus funciones y responsabilidades diarias. Por ello, cuando se utilice servicios de email y mensajería instantánea de la CFSE, todo usuario debe:

    a. Solo utilizar los servicios de email, mensajería instantánea y sus aplicaciones para enviar cualquier información relacionada a la CFSE.

    b. Asegurar que la información confidencial de la CFSE no pueda ser leída ni ojeada por ninguna otra persona mientras lea o escriba en lugares públicos.

    c. Utilizar herramienta encriptada aprobado por la CFSE y el personal de la Oficina de Sistemas de Información, cuando se envié información restringida o sensitiva.

    d. Borrar, sin abrir, cualquier mensaje o documento anejado de cualquier remitente desconocido, sospechoso, o desconfiable.

    e. Solo utilizar los equipos y dispositivos que llenen los requisitos de seguridad de la CFSE, según requiera cada uno de sus programas.

    f. Obtener autorización para enviar cualquier comunicación en masa (el mismo mensaje a una gran cantidad de personas). Ningún empleado y/o contratista está autorizado a enviar mensajes en masa, sin la debida autorización de la Oficina de Sistemas de Información.

    g. Reportar inmediatamente cualquier actividad sospechosa o cualquier incidente de seguridad relacionado al uso de email, mensajería instantánea, etc. a su supervisor

inmediato, el personal de sistemas de información y a las autoridades pertinentes dentro de la CFSE.

9. El uso del internet y los correos electrónicos pueden generar responsabilidad a la CFSE y al Gobierno de Puerto Rico. Por ello, todo usuario tiene prohibido:

    a. Enviar o recibir de mensajes de correo electrónico entre empleados de la CFSE y otras personas ajenas a esta en los cuales divulguen, comenten, o expresen hechos, opiniones, situaciones o asuntos internos de la CFSE que puedan poner en entredicho su reputación o imagen.

    b. Utilizar los sistemas de información y/o correo electrónico para difundir información ilegal, amenazante, fraudulenta, ofensiva, discriminatoria, sexualmente explícita, obscena, intimidante, irreverente, o difamatoria.

    c. Utilizar los sistemas de información y/o correo electrónico para enviar información o material que no sea oficial, mensajes en cadena, material político partidista o cualquier otra información o material ajeno a las funciones de la CFSE, o que no haya sido autorizado.

    d. Falsificar direcciones de email o mensajería instantánea, o enviar mensajes bajo el nombre de otro individuo u organización.

    e. Reenviar mensajes a personas fuera de la CFSE, incluyendo el reenviarlo a su email personal, sea de la CFSE o no.

    f. Generar copias de mensajes que contengan información sensitiva o restringida de la CFSE.

    g. Retener o copiar mensajes que contengan información interna de la CFSE de cualquier tipo, luego de una separación de su empleo bajo cualquier circunstancia.

h. Enviar información restringida de la CFSE mediante ningún servicio de email o mensajería instantánea.

i. Usar su servicio de email o mensajería instantánea personal para enviar información de la CFSE, con la excepción que algún funcionario con autoridad determine que hay razones apremiantes para así hacerlo.

j. Utilizar su servicio de email o mensajería instantánea personal durante horas laborables.

k. Modificar la configuración del servicio de email y mensajería instantánea de la CFSE, incluyendo las configuraciones de seguridad, para evitar su responsabilidad o los requisitos de las políticas de la CFSE.

l. Acceder a información de una cuenta ajena sin autorización, mediante la modificación de privilegios de acceso o la interceptación de información en cualquier otra manera.

F. Acceso y Solicitud de Acceso

1. Todo usuario accederá a los sistemas de información mediante cuentas que permitan establecer claramente su identidad y su nivel de acceso aprobado.
2. Se prohíbe el uso de cuentas anónimas o de invitado (guest, anonymus, u otro).
3. El empleado y/o contratista es responsable de proteger, recordar, guardar y asegurar sus claves de accesos y contraseñas, y puede ser responsable de cualquier daño que surja por el manejo negligente de sus claves de acceso y contraseñas.
4. Se prohíbe a los empleados compartir sus claves de accesos y contraseñas con otros empleados o cualquier otra persona interna, externa, relacionada o no a la CFSE.
5. El empleado que comparta su contraseña, use/maneje inadecuada o negligentemente su contraseña, no tome o deje de tomar las debidas precauciones o medidas para proteger su contraseña, de

otros empleados o de terceros, podrá ser referido a la Oficina de Relaciones Laborales y podría conllevar la imposición de sanciones administrativas, disciplinarias y hasta de índole legal, según aplique.

6. El contratista que comparta su contraseña, use/maneje inadecuada o negligentemente su contraseña, no tome o deje de tomar las debidas precauciones o medidas para proteger su contraseña de otros empleados o de terceros, será referido a las oficinas o agencias pertinentes para la posible cancelación del contrato y acción correspondiente.
7. Toda solicitud de creación, cambio, o cancelación de acceso a los recursos de información o sistemas lógicos de la CFSE debe ser originada por el director o supervisor de la oficina que la solicite. Se debe solicitar mediante el formulario CFSE 12-001, Solicitud para la Creación, Cancelación, o Sustitución de Contraseñas.
8. Cuando un director o supervisor solicite un acceso para un empleado, el personal autorizado de la OSI evaluará la solicitud y otorgará el acceso, siempre que corrobore que las funciones del puesto así lo requieren.
9. El Director del Área de Recursos Humanos deberá notificar por escrito al Director de Sistemas de Información sobre el reclutamiento, transferencia, jubilación, despido, o renuncia de cualquier empleado, no más tarde de 30 días de ocurrir el cambio.
10. La OSI es responsable de inactivar inmediatamente el acceso de todo empleado a la fecha de terminación de su empleo en la CFSE.
11. Los accesos otorgados serán los mínimos que necesite el empleado o funcionario para el desempeño de las tareas requeridas para su posición.

G. Utilización de Contraseñas

1. Todos los accesos a los programas o aplicaciones de las operaciones de la CFSE deberán tener controles de acceso para su utilización, de modo que solo el personal autorizado pueda ver datos o acceder aplicaciones que necesite usar, por lo que estarán protegidos y serán controlados mediante mecanismos que requieran el nombre de usuario (user name) y una contraseña o código de acceso (password) para la autenticación y autorización de accesos.
2. La OSI asignará el nombre de usuario y establecerá los requisitos mínimos para el uso y protección de contraseñas.
3. Las contraseñas deben consistir de una combinación de números, letras, y caracteres especiales, que entre ellos tenga un mínimo de ocho (8) caracteres.
4. La OSI proveerá los medios para que las contraseñas que cada usuario utilice para acceder los sistemas de la CFSE se actualicen periódicamente. En el caso de administradores: mínimo cada cuatro (4) meses; en el caso de usuarios: mínimo cada seis (6) meses.
5. Las contraseñas serán mantenidas en estricta confidencialidad y cada empleado es responsable de mantener sus claves de acceso protegidas en todo momento y tomar todas las medidas necesarias para evitar que terceras personas tengan acceso a las mismas.
6. El uso de una contraseña o un código de acceso (password) para tener acceso a los sistemas de información o programas de la CFSE no será obstáculo para que se realicen auditorías al sistema cuando sea necesario o requerido.
7. El usuario no alberga una expectativa de intimidad alguna con relación a la información almacenada en los equipos que le haya asignado la CFSE o en cualquier programa o aplicación instalada a tales efectos.

8. Las contraseñas utilizadas para proteger información confidencial o clasificada deben estar adecuadamente estructuradas, protegidas y deben ser cambiadas de acuerdo con el uso de cada contraseña o según establezca La OSI.
9. Los estándares para el uso y manejo de las contraseñas aplican a todas las contraseñas utilizadas para acceder, modificar o proteger información confidencial o clasificada de la CFSE, o contraseñas utilizadas para acceder o modificar información de la CFSE accesibles a través de cualquier red.
10. Las contraseñas exclusivas de un individuo no deberán ser compartidas a otros individuos o usuarios.
11. Se recomienda que ninguna contraseña utilizada dentro de la CFSE deberá ser utilizada para aplicaciones, programas o accesos externos.
12. Los sistemas no deberán tener facultades para almacenar contraseñas, a menos que sea necesario para las operaciones de la CFSE, en cuyo caso, el sistema deberá está protegido de acceso indebido a las contraseñas.

H. Tecnologías en la Nube (Cloud Computing)

1. La adquisición y utilización de Tecnologías de Nube deberá estar autorizada formalmente por los mismos mecanismos aplicables a otros servicios de informática que involucran a la ATI.
2. La solicitud de autorización de Tecnologías de Nube deberá estar acompañada de un formulario de evaluación específico para el tipo de servicio (Evaluación de Tecnologías en la Nube).
3. La utilización de Tecnologías en la Nube deberá cumplir con todas las leyes y reglamentos de privacidad y confidencialidad aplicables a nivel estatal y federal. La agencia que adquiera los servicios de Tecnologías en la Nube será responsable por asegurar que los roles y responsabilidades relacionadas al manejo de datos y la privacidad y confidencialidad de los mismos están clara y

adecuadamente definidos en el acuerdo de servicio del proveedor de Tecnologías en la Nube.

4. El acuerdo de servicio del proveedor de Tecnologías en la Nube deberá ser remitido a ATI para su evaluación y aprobación. De existir un el servicio mediante contrato global suscrito por ATI, la OSI y/o la CFSE deberá justificar la razonabilidad y costo-efectividad de la contratación directa.

5. La OSI deberá justificar la necesidad de utilizar un servicio de Tecnologías en la Nube que incluya alguna de los siguientes atributos:

    a. Mayor eficiencia o efectividad en la prestación de un servicio tecnológico.

    b. La necesidad de un atributo específico de tecnologías de nube (ej. elasticidad, escalabilidad, modelo basado en utilización).

    c. La necesidad de establecer un servicio tecnológico en un periodo corto de tiempo.

    d. La necesidad de establecer nuevos o mejores mecanismos de contingencia, recuperación de desastres o estrategias para garantizar la continuidad del negocio.

    e. La necesidad de establecer como estrategia, ambientes de desarrollo, prueba, control de calidad, o cualquier otra necesidad cónsona con las mejores prácticas en el ciclo de desarrollo de software.

6. La CFSE mantendrá un récord exacto de los costos asociados con el ciclo de vida de la solución de la Tecnología de Nube, desde su implementación, mantenimientos, reparaciones, y descontinuación, y cualquier otra etapa de su vida útil que genere algún costo para la CFSE.

7. La CFSE deberá consultar con ATI al comienzo de cada ciclo de evaluación de Tecnologías de Nube para determinar si existen

contratos o acuerdos en el Gobierno de Puerto Rico que puedan ser aprovechados o consultados para el proyecto.

8. La OSI debe realizar un análisis de riesgo completo previo a contratar cualquier servicio para Tecnologías de Nube, que incluirá el solicitar evidencias al proveedor sobre las evaluaciones de riesgos practicadas al servicio de Tecnologías de Nube.
9. La OSI debe establecer procedimientos para informar incidentes, obtener respuestas de parte del proveedor, y cualquier función de seguridad necesaria que se realice con el proveedor.
10. La OSI debe establecer un plan de migración en caso que haya que cambiar de proveedor de solución de Tecnologías en la Nube o desee traer la solución a la infraestructura tecnológica de la CFSE, o vice versa, y así evitar estar atados a una sola solución.
11. La OSI debe conocer y orientar a los funcionarios, empleados, contratistas y usuarios de los sistemas de información sobre sus roles y responsabilidades relacionadas a la implantación, operación y apoyo de la solución de Tecnologías de Nube.
12. Al elegir la Tecnologías de Nube a implementarse en la CFSE se deben tomar en consideración los siguientes aspectos técnicos:
    a. Implementar y utilizar estándares, formatos, y protocolos abiertos, o en la alternativa, se deberán establecer y garantizar mecanismos para la recuperación de datos.
    b. Dar prioridad a quienes provean mecanismos para desarrollar, extender, y mejorar la funcionalidad base que proveen sus servicios.
    c. Dar prioridad a quienes provean componentes y servicios que estén basados o se puedan extender utilizando tecnologías abiertas.
    d. Dar prioridad a quienes cuentan o colaboran con proyectos con la capacidad para replicar la implementación de la nube utilizando la estructura de la CFSE.

I. **Conexión Remota (Red Virtual Privada o Virtual Private Network)**

1. El empleado que desee conectarse remoto desde las computadoras o la red de la CFSE a su computadora privada deberá fundamentar su solicitud por escrito y será evaluada y autorizada por el Director de Sistemas de Información.
2. Al conectarse remoto, el empleado autorizado podrá tener acceso a información confidencial de la CFSE, de empleados y de terceros, por lo que deberá hacer uso adecuado y proteger dicho privilegio, incluyendo salvaguardar los códigos o claves de acceso, y será responsable por cualquier daño que su incumplimiento con la política ocasione a la CFSE, a los empleados o a terceros.
3. La OSI definirá y actualizará periódicamente los estándares de conexión a la red desde cualquier punto para minimizar la exposición a posibles daños, incluyendo conexiones de Dial-Up, Virtual Private Network (VPN), o cualquier otra tecnología útil para este propósito.

J. **Aplicaciones de Servicio**

Todo programa de aplicación desarrollado para la CFSE deberá contar con los siguientes elementos en su estudio de viabilidad para su implementación:

a. Diseño de seguridad.
b. Integración de mejores prácticas de seguridad en programación para evitar el acceso no autorizado y/o malicioso a través de cualquier red.
c. Un firewall que permita controlar el acceso a los programas desde internet.
d. Si la aplicación o sistema maneja datos sensitivos, utilizar una red alterna segura que permita acceso al internet y permita un acceso controlado a la red interna para el intercambio controlado y monitoreado de datos.

e. Un sistema de detección y prevención de intrusos si la aplicación tiene acceso al internet.

K. Disposición de Equipos e Información

1. La OSI será responsable de disponer adecuadamente de todo equipo electrónico para el cual no se tenga uso o haya culminado su vida útil para evitar el mal uso del equipo y proteger la confidencialidad de los datos contenidos en los mismos.
2. La OSI establecerá y documentará los procedimientos de seguridad para la disposición de equipos, programas, aplicaciones, y periferales propiedad de la CFSE.
3. Se prohíbe la donación, regalo, cesión, reventa, o la transferencia de cualquier modo de equipo propiedad de la CFSE, este en uso, desuso, así se determine o no que es útil o necesario sin previa autorización.
4. Para cumplir con esta política, la OSI deberá:
    a. Sustituir o eliminar permanentemente servidores, consolas, computadoras, dispositivos, programas y aplicaciones existentes que hayan culminado su vida útil.
    b. Resguardar (back-up), restaurar y mantener bases de datos, configuración de archivos y documentación que se encuentre almacenada en los equipos, programas, o aplicaciones a disponer.
    c. Actualizar versiones y aspectos de seguridad a considerar en los recursos de información.
    d. Crear y mantener una lista de control de los periferales, programas y aplicaciones a disponer o actualizar.
    e. Remover toda información de todo equipo y programación a través de un proceso remoción de su contenido, previo a su destrucción, utilizando el método de remoción más adecuado, según determine el Director de la OSI.

f. Destruir los equipos que no se reutilizaran, utilizando el método de destrucción más adecuado, según determine el Director de la OSI.

g. Remover las licencias que contenía el equipo, las cuales permanecerán en un inventario de licenciamiento.

h. Emitir una certificación que indique que los equipos no contienen información de la CFSE y son inservibles u obsoletos.

i. Seleccionar una compañía certificada para realizar el decomiso.

j. Proveer a la Oficina de Auditoría Interna la información de los equipos a decomisar.

k. Requerirá personal de la Oficina de Auditoría Interna para el proceso de decomiso y certifique que se haya llevado a cabo, según la reglamentación vigente.

L. Cuentas Inactivas

1. La OSI tiene la responsabilidad de monitorear las cuentas definidas en los sistemas.
2. La OSI deberá deshabilitar toda cuenta que se encuentre inactiva durante el periodo de un año.

M. Protección y Cuidado de Equipos de Periferales

1. Los equipos y computadoras de la CFSE serán instalados y configurados exclusivamente por el personal autorizado por la OSI. Ningún usuario está autorizado a realizar tareas de instalación de equipo, conexiones a la red, programas o software ni de reparación.
2. El usuario que detecte o sea informado de un problema en el funcionamiento del sistema deberá notificarlo de inmediato a la OSI.

3. Solo el personal de la OSI está autorizado para revisar los equipos de la CFSE, corregir cualquier falla en los equipos o sistemas de información, o referir la situación para reparación.
4. Cualquier movimiento de equipo o periferales deberá ser aprobado por y coordinado con la OSI.

N. Manejo y Documentación de Incidentes, Problemas y Peticiones

1. La OSI preparará y actualizará periódicamente un plan para el manejo de incidentes y problemas relacionados a los sistemas de información de la CFSE.
2. El plan para el manejo de incidentes y problemas servirá de guía para recomendar, coordinar, y documentar acciones de mitigación inmediatas en caso de que ocurra algún evento inesperado en los recursos de los sistemas de información.
3. Los empleados de la OSI deben conocer el plan para el manejo de incidentes y problemas; y seguir los procedimientos en vigor para evitar que afecten la seguridad e integridad de los recursos de informática.

O. Política sobre el Servidor de Seguridad de Computadoras y Redes (Firewall)

1. Los sistemas de información de la CFSE estarán protegidos por un firewall.
2. Si el firewall requiere una licencia, la OSI deberá asegurar que la misma está vigente.
3. La OSI deberá realizar resguardos de la configuración del firewall, cuyo acceso estará restringido al personal de la OSI.
4. El personal de la OSI deberá estar adiestrado en el manejo, instalación y revisión de firewalls.
5. Las reglas mínimas que debe tener los firewalls son los siguientes:
    a. Firewalls perimetrales:

i. Denegar todo tráfico que no esté explícitamente permitido en ambas direcciones (inbound and outbound).

ii. Permitir tráfico de salida (outbound) solo en puertos que se utilizan.

b. Filtros de contenido de internet deben poseer al menos un filtro que bloquee pornografía y material no permitido, que aplique a todo el personal.

P. Monitoreo de los Sistemas Tecnológicos y Pruebas de Control y Vulnerabilidad

1. La OSI es responsable de la protección de los sistemas de información incluyendo equipos de computadoras, servidores y todo lo relacionado a comunicaciones de Voz y Data. Para esto, en todas las facilidades de la CFSE existe un espacio físico el cual debe mantenerse con acceso restringido estableciéndose unos requisitos mínimos de seguridad. También se debe mantener un registro de quienes entran y salen de dichas facilidades con fecha, nombre, oficina y propósito. De ser necesario el acceso a dicho lugar, por personal ajeno a la OSI, debe mediar una autorización previa de ésta oficina.
2. La CFSE se reserva el derecho de auditar, vigilar y fiscalizar los sistemas de correspondencia electrónica y todos los servicios computadorizados para garantizar que su propiedad sea utilizada solo para propósitos y gestiones relacionadas con el trabajo, certificar la seguridad e integridad de sus sistemas y equipos, y evitar la divulgación no deseada y la pérdida de información.
3. La CFSE puede realizar auditorías periódicas, según lo determine el Director de la OSI o el Administrador, o cuando exista una investigación sobre alguna situación que amerite dicha auditoría.
4. La OSI establecerá las herramientas y medidas de seguridad para monitorear la actividad de la red corporativa externa e interna, las

bases de datos, los aplicativos, los servidores, el internet, y el correo electrónico. El monitoreo de los recursos informáticos será continuo e incluirá:

a. Investigación de Fraude
b. Monitoreado por la Oficina de Seguridad de TI
c. Interferencia
d. Pérdidas de la conexión
e. Accesos no autorizados
f. Registro de eventos (Log events)
g. Manipulación del registro de seguridad
h. Réplica de archivos (File replication)
i. Sistema de nombres de dominio (Domain Name System o DNS)
j. Controles de dominios
k. Pistas de auditoria (Audit Trails [Transactional and Security])
l. Correo no deseado (Spam)

5. La OSI designará el personal interno o externo para realizar evaluaciones de vulnerabilidad (vulnerability assessment) o las pruebas de intrusión al sistema.
6. Todos los resultados y acciones de remediación deben ser documentadas por el personal ejecutor y notificados al Director de OSI para evaluación.
7. La OSI deberá gestionar una evaluación de riesgos para determinar el valor de la información y el impacto de la pérdida, modificación, alteración o divulgación no autorizada de la información de la CFSE.
8. La OSI deberá verificar que el sitio web cuenta con todos los mecanismos en vigor para protección adecuada para la información de la CFSE.
9. La OSI deberá realizar análisis de riesgo, pruebas de vulnerabilidad y penetración para determinar si el portal principal

debe ser puesta en suspenso por un tiempo, considerando la importancia de que la misma se mantenga activa.

10. La CFSE deberá mantener sus recursos de computación y comunicaciones seguros y protegidos de programas maliciosos en todo momento.
11. El monitoreo, escaneo y evaluación, así como el colocar en cuarentena o confiscación de cualquier dispositivo que acceda las redes y sistemas de información de la CFSE debe cumplir con todas las leyes y reglamentos locales y federales aplicables.
12. La CFSE se reserva el derecho de escanear los recursos de comunicación para identificar la presencia de programas dañinos como virus, malware, spyware, etc., en cualquier momento, y monitorear o revisar el contenido y patrones de tráfico, incluyendo cualquier actividad o tráfico que se origine remotamente. La evaluación y monitoreo podrá realizarse para mantenimiento del sistema, detectar y eliminar alguna contaminación, detección y prevención de divulgación de información sensitiva de la CFSE, detección de accesos no autorizados a las redes y sistemas de información, y para evaluar el cumplimiento con las políticas de la CFSE y el Gobierno de Puerto Rico.
13. La CFSE se reserva el derecho de bloquear y eliminar emails y/o sus anejos de entrar o salir de las redes de la CFSE basado en su sujeto, contenido, remitente, o receptor del email.
14. La CFSE se reserva el derecho de colocar en cuarentena o confiscar todo dispositivo, equipo o recurso de cualquier tipo que pueda ser una amenaza para la CFSE. Si de cualquier evaluación surge la sospecha de actividad criminal, la CFSE referirá el asunto a las autoridades, cooperando con toda investigación y proveyendo toda evidencia y testimonio necesario, y tomará la acción legal pertinente.

15. La OSI se reserva el derecho de desconectar de sus redes y sistemas de información cualquier dispositivo que este o se sospeche que no está adecuadamente protegida por algún programa antimalware aprobado o aceptado. Cualquier dispositivo removido que interese ser reconectado al sistema debe demostrar que está en cumplimiento con las políticas de seguridad de las redes y sistemas de información de la CFSE.
16. Los equipos y sistemas de información deberán mantener siempre instalado un programa comercial antiwalware, configurado apropiadamente y operando en todo momento.
17. Los programas antimalware deberán configurarse adecuadamente, de modo que protejan efectivamente contra toda amenaza conocida.
18. Ningún empleado deberá desactivar los programas anti-malware instalados en los equipos, periferales y sistemas de información de la CFSE. Solo la OSI está autorizado para desactivar brevemente el programa anti-malware para apoyar la instalación de un programa autorizado.
19. La OSI deberá asegurar que existe en vigor un mecanismo para verificar que el programa anti-malware fue reinstalado y que se cumpla con dicho procedimiento o protocolo.
20. La OSI deberá instalar actualizaciones al antimalware sin que lo inicie o intervenga el usuario.
21. La OSI deberán poner en vigor una política escrita para la instalación de nuevas actualizaciones de seguridad, incluyendo actualizaciones al motor de escaneo de los programas antimalware.
22. La OSI se asegurará de limitar los accesos a los espacios físicos que contienen equipo que procese, almacene, contenga o que de algún modo pueda afectar información sensitiva de su propiedad.

Q. Programa de Continuidad

1. La OSI deberá establecer un plan para apropiadamente responder, monitorear y reportar incidentes relacionados a la seguridad de la información conocidos o sospechados. Además, deberá instituir y practicar un plan para la continuidad de los negocios y recuperación en caso de desastre de sistemas de información para la prevención de pérdida catastrófica de información y asegurar la restauración oportuna de las redes y sistemas de información en el evento de algún daño, destrucción o falla en el sistema.
2. El Director de la OSI será la persona designada como Líder de Tecnología en el Comité de Continuidad Gubernamental, responsable del desarrollo y ejecución del Plan de Recuperación de Desastres.
3. La OSI deberá realizar un análisis de riesgos cada 12 meses y un análisis de impacto al menos cada 24 meses, o luego de cualquier cambio significativo en la infraestructura operacional.
4. La OSI deberá establecer un Plan de Recuperación de Desastres donde establezca las estrategias en respuesta, recuperación, reanudación y restauración de los procesos críticos de las unidades de la CFSE, tanto a nivel de las plataformas de procesamiento y de sus comunicaciones.
5. La CFSE deberá contar con un Plan de Manejo de Incidentes donde establezca los procedimientos para detectar reportar, y responder a cualquier tipo de incidente que cause interrupción en las operaciones de la CFSE.
6. Esta política representa los requisitos mínimos para el contenido de un plan para que asegure la continuidad de los negocios y recuperación en caso de desastre de sistemas de información, y su enfoque debe estar en sus activos de información crítica.

R. Control Ambiental de los Recursos de Informática

1. La OSI implementará controles ambientales (environmental controls) en las áreas donde se encuentren los recursos informáticos con el propósito de prevenir, detectar, y reaccionar a condiciones perjudiciales tanto para el personal de la CFSE como para el equipo.
2. Estos controles incluyen, pero no se limitan a, aires acondicionados, extintores de incendio, alarmas de fuego, sensores de calor, generadores de energía, suelo técnico, controles de temperaturas, cámaras de vigilancia y puertas de emergencia.

S. Boletín Informativo de Medidas de Seguridad

La OSI y la Oficina de Información Pública prepararán y promulgarán boletines informativos para orientar a los empleados y/o contratistas sobre el uso adecuado de los sistemas tecnológicos y educar sobre las medidas de seguridad necesarias para evitar riesgos a los sistemas y la información almacenada en los mismos, y fraude cibernético en todas sus modalidades.

T. Cumplimiento de Política

1. Esta política aplica a todos los sistemas de computadoras, que incluye todas las computadoras de escritorio, computadoras portátiles, estaciones de trabajo, o servidores que acceden, procesan o transmiten información de la CFSE y a dispositivos móviles con acceso a la red de la CFSE de cualquier modo.
2. La OSI deberá adoptar los procedimientos internos necesarios para garantizar el fiel cumplimiento con las disposiciones de este Reglamento.
3. La CFSE promoverá el buen uso y manejo de sus equipos de información, así como el cumplimiento de la normativa establecida sobre la seguridad de los recursos de informática.

4. La violación evidenciada conllevará la imposición de medidas disciplinarias, según provee el Manual de Normas de Conducta y Medidas Disciplinarias de la Corporación del Fondo del Seguro del Estado; así como la presentación de cualquier recurso legal que corresponda ante la agencia o tribunal estatal o federal pertinente, o el referido a las autoridades de ley y orden pertinentes, tales como el Buró Federal de Investigaciones (FBI), y la Policía de Puerto Rico.
5. El incumplimiento con estas políticas puede resultar también en la eliminación de sus accesos y privilegios en el CFSE, sus redes, equipos y sistemas.
6. La CFSE se reserva el derecho de monitorear el tráfico y contenido (dentro, fuera, remoto, o en dispositivos de almacenaje) y revisar las redes y sistemas para evaluar toda actividad utilizando los recursos de la CFSE. Dicho monitoreo será con el propósito de asegurar el cumplimiento con esta política, y respetando las leyes federales y locales, así como los derechos de privacidad de los individuos.

ARTÍCULO VIII – SALVEDAD

"Si cualquier artículo, inciso, párrafo, o parte de este documento fuere declarado nulo por un tribunal con competencia, dicha declaración de nulidad, no afectará las demás disposiciones del mismo, las cuales continuarán vigentes."

ARTÍCULO IX – DEROGACIÓN

Este Reglamento deroga la **OA 16-05, Orden Administrativa para Establecer la Política Institucional Referente al Uso Adecuado de los Sistemas de Informática y Equipos Tecnológicos de la CFSE** de **26 de marzo de 2016**.

ARTÍCULO X – APROBACIÓN

Este Reglamento fue aprobado por la Junta de Gobierno de la Corporación del Fondo del Seguro del Estado, mediante la Resolución Número **A-68-2019** del **22 de octubre de 2019.**

ARTÍCULO XI - VIGENCIA

Este documento tendrá vigencia a partir de su aprobación, firma y radicación en el Departamento de Estado del Gobierno de Puerto Rico.

Jesús M. Rodríguez Rosa, MIS
Administrador