Número: *8436*
Fecha: 8 de enero de 2014
Aprobado: Hon. David E. Bernier Rivera
Secretario de Estado

Por: Francisco J. Rodríguez Bernier
Secretario Auxiliar de Servicios

ESTADO LIBRE ASOCIADO DE PUERTO RICO
OFICINA DEL COMISIONADO DE INSTITUCIONES FINANCIERAS
SAN JUAN, PUERTO RICO

Reglamento para el Uso y Control de los Equipos y Sistemas de Información

ÍNDICE

CONTENIDO **PÁGINA**

ARTÍCULO 1. Título

Este reglamento se conocerá como **"Reglamento para el Uso y Control de los Equipos y Sistemas de Información" (en adelante, "Reglamento")**.

ARTÍCULO 2. Base Legal

Este **Reglamento** se promulga y adopta en virtud la facultad conferida al Comisionado de Instituciones Financieras en la Ley Número 4 de 11 de octubre de 1985, según enmendada, conocida como "Ley de la Oficina del Comisionado de Instituciones Financieras", y en armonía con la Ley Número 170 de 12 de agosto de 1988, según enmendada, conocida como "Ley de Procedimiento Administrativo Uniforme del Estado Libre Asociado de Puerto Rico", según enmendada, para promulgar los reglamentos y procedimientos que sean necesarios para el mejor desempeño de sus funciones. La Ley Núm. 4 dispone en su Artículo 8 que el Comisionado, ".....tendrá poderes y facultades para: reglamentar sus propios procedimientos y normas de trabajo".

Además, este **Reglamento** se adopta en armonía con la Ley sobre Derechos de Autor, según enmendada, conocida como Ley sobre Derechos de Autor ("Copyright Act of 1976") del 19 de octubre de 1976; la Ley Núm. 96 del 15 de julio de 1988, según enmendada, conocida como "Ley de Propiedad Intelectual de Puerto Rico"; la Ley Núm. 151 del 22 de junio de 2004, conocida como "Ley de Gobierno Electrónico"; la Carta Circular Núm. 77-05 de 8 de diciembre de 2004 de la Oficina de Gerencia y Presupuesto; Política Núm. TIG-008; la Política Núm. TIG-018 de 1 de abril de 2013 de la Oficina de Tecnologías de Información Gubernamental de la Oficina de Gerencia y Presupuesto; el Reglamento Núm. 3381 "Reglamento de Adquisición", de 2 de diciembre de 1986, según enmendado, que regula la adquisición de bienes y servicios no profesionales por la Rama Ejecutiva; el Reglamento Núm. 11, y las "Normas Básicas para el Control y Contabilidad de los Activos Fijos", de 8 de abril de 2002, según enmendado.

ARTÍCULO 3. Política y Propósito

La Oficina del Comisionado de Instituciones Financieras ("OCIF") tiene la obligación de asegurar la integridad y exactitud de la información de la agencia, protegiéndola contra la divulgación, manipulación, modificación o destrucción no autorizada o accidental. Tanto los equipos de computadoras, los programas ("software"), así como la información contenida en el banco de datos de la OCIF ("data base"), son propiedad de la OCIF por lo que los empleados, consultores y contratistas deben tomar las medidas necesarias para salvaguardar la disponibilidad, integridad y confidencialidad de los datos que sus sistemas de tecnología manejan.

Conforme a este **Reglamento**, la OCIF requiere que su personal utilice correctamente los equipos de computadoras, así como los programas y todas las piezas o aditamentos que se conecten a éstos (periféricos) y que complementan su funcionamiento. El personal tiene el deber de tomar las medidas necesarias para proteger el equipo y asegurar su funcionamiento

óptimo.

Para ello, este **Reglamento** promulga y establece las normas que regirán la adquisición y utilización adecuada de las computadoras, los periféricos y demás equipo, las aplicaciones comerciales y los programas desarrollados internamente; consigna las medidas de control para la protección del mismo; expide las normas para controlar el acceso a los programas y documentos; y determina los mecanismos adecuados para el almacenamiento y protección de documentos tales como el archivos de información regular y confidencial e informes relacionados, archivos de información en casos de desastre y discos removibles de información.

Además, este **Reglamento** establece una política que garantiza el buen uso, manejo, administración de los recursos de Internet así como la mensajería electrónica, para que constituya un instrumento suplementario que permita al personal enviar o buscar información de una manera más eficiente.

Mediante este **Reglamento** se uniforman en un solo documento todas las normas emitidas por la OCIF relacionadas a sistemas de información, y por tanto las mismas en su forma individual quedan sin efecto. Estas son: el Manual del Usuario del Comité de Mejoramiento Sistemas Electrónico y de Información de 3 de septiembre de 1996 emitido por la OCIF; el Memorando de 23 de junio de 1997 sobre Cambios y utilización de las claves de acceso ("passwords"); el Manual del Usuario-Normas para el Uso de Computadoras y Telecomunicaciones de 27 de agosto de 1997; el Manual de Políticas para el Uso del Correo Electrónico de 30 de mayo de 2002; las Normas para la Protección Antivirus de 24 de junio de 2002; los Procedimientos sobre Resguardo (Backups) de los Programas y Bases de Datos y Custodia de las Cintas de 26 de febrero de 2007; y la Orden Administrativa de la OCIF 3-12 sobre el Uso del Correo Electrónico de 7 de junio de 2012.

ARTÍCULO 4. Alcance

Este **Reglamento** aplica a todos los empleados de la OCIF sin importar el nivel o jerarquía. De igual forma, aplica a cualquier personas no empleadas por la OCIF, tales como: aspirantes a empleo, consultores, contratistas o sus representantes, o terceras personas no empleadas por o ajenas a la OCIF que utilicen equipos electrónicos computadorizados que por la naturaleza de su contrato o de su relación necesite utilizar las herramientas que se describen en este **Reglamento**.

ARTÍCULO 5. Definiciones

Los siguientes términos tienen el significado que a continuación se expresa:

1. **Acceso remoto:** Es el acceso desde una ubicación fuera de la red de la OCIF a los funcionarios, empleados o contratistas que están sujetas a los requisitos de acceso autorizado.

2. **Acoso cibernético (intimidación cibernética, ciberacoso o "Cyberbullying")**: Significará un acto o patrón de incidentes donde medie la transmisión de cualquier tipo de comunicación electrónica, oral, escrita, visual o textual, con el propósito de acosar, intimidar, hostigar y afligir a una persona o grupo de personas, ocasionando o intentando ocasionar con dicho comportamiento: (1) interferencia en las oportunidades, desempeño y beneficios de la persona en su trabajo, vida familiar o social; (2) provocarle daño físico, mental y emocional a la persona o destrucción de su propiedad o llevarle a auto-infligirse tal daño; (3) poner de manera consciente a la persona, en una posición en la cual razonablemente sienta temor por su seguridad física o daño a su propiedad o a sus allegados; (4) cree un ambiente laboral hostil o provoque agresiones por terceras personas. Será indiferente que el provocador actúe como uno mismo, o haciéndose pasar por otra persona, sea real o ficticia, o pseudónimo. El "cyberbullying" se manifiesta en distintas formas incluyendo "flaming" o peleas en línea mediante mensajes electrónicos con lenguaje vulgar u ofensivo; acoso repetido de envió de mensajes crueles, viciosos o amenazantes; denigración al enviar o publicar chismes o rumores crueles acerca de una persona para dañar su reputación; suplantación al irrumpir en la cuenta de correo electrónico de alguien y usarlo para enviar material vicioso o embarazoso a otros; salida y engaño comprometiendo a alguien en la mensajería instantánea, engañando a él o ella en revelar información sensible y reenviar la información a los demás; exclusión intencional a alguien de un grupo en la línea; y "outing" compartir secretos, información e imágenes embarazosas de alguien en línea.

3. **Administrador del Sistema de Correo Electrónico:** Será un empleado del Área de Sistemas de Información o algún recurso asignado por el Director del Área de Sistemas de Información o el Comité de Tecnología que se encargara de la administración y soporte del Sistema de Correo Electrónico de la OCIF.

4. **Antivirus**: Programa que se utiliza para evitar que un virus haga daño a la computadora, aplicaciones o información dentro de la computadora.

5. **Aplicación**: Conjunto de instrucciones que permiten procesar datos a través de funciones de cálculo, movimiento de un lado a otro en memoria, comparaciones y otros, con el propósito de obtener unos resultados esperados. Estas son desarrolladas por los analistas de sistemas o adquiridas comercialmente pre-programadas y se utilizan para cumplir con los propósitos establecidos en este **Reglamento**.

6. **Archivo o "file"**: Conjunto de datos almacenados en un formato en específico. Puede ser una información de texto, hojas de cálculos, gráficas, imágenes, fotografía, bases de datos o cualquier otro conjunto de datos guardado en cualquier equipo.

7. **Área de Sistemas de Información**: Área de Sistemas de Información de la OCIF compuesto por algunos empleados relacionados a los servicios de sistemas de información, el Principal Oficial de Informática y el Comisionado Auxiliar del Área de Administración. Incluye a los contratistas especializados bajo dicha materia que responden directamente al Comisionado.

8. **Asecho cibernético ("Cyberstalking")**: significará participar o llevar a cabo conducta para comunicarse, o para hacer que se comuniquen, palabras, imágenes, lenguaje, o por medio de la utilización del correo electrónico, comunicación electrónica, o equipos cibernéticos dirigida a una persona, causando considerable angustia emocional y/o física a esa persona.

9. **Autenticación**: Identidad de quien envía el mensaje.

10. **Base de Datos:** Es el almacenamiento e integración colectiva de datos e información que son requeridas por organizaciones para cubrir sus requisitos de procesamiento.

11. **"Chat"**: Programa de mensajería interactiva. Comunicación entre dos usuarios a través de la computadora en tiempo real.

12. **Cifrar (Encryption):** Proceso en el cual los datos se convierten a un formato que no se puede descifrar fácilmente por personas no autorizadas a acceder los mismos.

13. **Clave, contraseña o "password" de acceso**: Clave particular e intransferible de cada usuario para registrarse en la computadora y lograr acceso a la red u otras aplicaciones o bases de datos para poder interactuar y acceder información en el medio computadorizado.

14. **Código fuente (Source Code)**: El **código fuente** de un programa informático (o software) es un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa. Por tanto, en el código fuente de un programa está escrito por completo su funcionamiento.

15. **Comisionado**: Significa el Comisionado de Instituciones Financieras de Puerto Rico.

16. **Comisionado Auxiliar o Director**: Todo funcionario o empleado de la OCIF que ejerce algún control o cuya recomendación sea considerada para la contratación, clasificación, despido, ascenso, traslado, fijación de compensación o sobre otras condiciones de trabajo, tales como horario, lugar de trabajo, tareas o funciones que desempeña o pueda desempeñar un empleado o grupo de empleados o sobre cualesquiera otros términos o condiciones de empleo, o cualquier persona que día a día lleve a cabo tareas de supervisión.

17. **Comité de Tecnología**: equipo de funcionarios, empleados o contratistas que se reúnen para discutir y asesorar al Comisionado en cuanto a los asuntos relacionados a Sistemas de Información.

18. **Comunicaciones**: Tipo de conexión de una computadora, la cual permite mantener contacto con otra computadora, aplicación, servidor o entre usuarios.

19. **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 OCIF. 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 de personas ajenas a la OCIF.

20. **Contratista**: Toda persona, natural o jurídica, sus representantes o empleados, que mantenga una relación contractual con la OCIF, incluyendo el personal por contrato de servicios misceláneos y los que laboren bajo contratos profesionales y consultivos.

21. **Copias ilegítimas**: Se refiere a cuando se realiza un duplicado idéntico de las aplicaciones comerciales o de las desarrolladas internamente sin la debida autorización del dueño o responsable del mismo.

22. **Correo Electrónico o "e-mail"**: Servicio de correspondencia mediante la transmisión de mensajes, archivos o datos relacionados con su trabajo en y fuera de la OCIF a través de la red de computadoras.

23. **Cuenta de Correo Electrónico**: Herramienta de trabajo y privilegio otorgado a un empleado o contratista dirigida a fomentar la buena comunicación y promover los niveles de excelencia en la ejecutoria, que deben prevalecer en toda entidad pública.

24. **Custodio y Custodio Alterno:** es la persona designada, ajena a la administración u operación diaria de los servidores, encargada del recogido, control y custodia de las cintas de respaldo.

25. **Custodio de la base de datos**: Es la persona responsable de la información que se encuentra en una base de datos o un representante autorizado. Como por ejemplo: la base de datos de Nóminas, es el Supervisor de la Sección de Nóminas y el encargado de la base de datos de la Oficina de Compras es el Supervisor de Compras o sus respectivos representantes autorizados.

26. **Data/datos**: Distintas piezas de una información.

27. **Derechos de Autor**: Ley aprobada por el Congreso de Estados Unidos conocida como Ley sobre Derechos de Autor, ("Copyright Act of 1976"), del 19 de octubre de 1976. La misma dispone entre otras cosas, la prohibición de hacer, duplicar, copiar, vender o distribuir programas o "software" con fines de lucro sin la debida autorización del autor, inclusive prohíbe el hacer copias múltiples destinadas al uso de varios usuarios dentro de la misma organización y dar copia ilegal a otro usuario. Las leyes de derechos de autor establecen responsabilidad civil, criminal y multas a quien lo viole.

28. **Documentación**: Consiste de la lista de códigos (lenguaje) y la prueba del programa, conjuntamente en la totalidad de los datos de la aplicación que se necesitan para entender lo que ejecuta la misma. Consistirá en diagramas de flujo, manual de programas, instrucciones, etc.

29. **"Drives":** Es un dispositivo que lee y/o escribe datos en un medio de almacenamiento como disquetes, discos ópticos, etc.

30. **Entorno**: Sistema operativo mediante el cual se ejecutan determinados programas en la computadora.

31. **Equipo**: Se refiere al equipo electrónico de la OCIF tal como, la computadora y todos sus componentes físicos o periféricos, como por ejemplo: host computers, desktops, monitor o pantalla, teclado, impresora, unidad de disco, batería, teléfono, facsímile, entre otros.

32. **Estación de Trabajo**: Se refiere al área en donde el usuario tiene el equipo asignado para su uso oficial.

33. **Funcionario o empleado**: Toda persona que ocupa un cargo o puesto en la OCIF, incluyendo empleados regulares, irregulares, transitorios, probatorios, candidatos a empleo preseleccionados y de confianza.

34. **Información:** es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado suceso.

35. **Información Confidencial**: Información que está protegida por las leyes del Estado Libre Asociado de Puerto Rico.

36. **Interceptación**: Cuando un mensaje es interceptado en cualquier punto no asegurado en el camino hacia el usuario final. La interceptación activa son expertos que entran al sistema sobrepasando la seguridad, lo que no solo compromete la confidencialidad de la información, sino también causa el riesgo potencial de robo de contraseñas.

37. **Internet**: Red de comunicaciones mundial, descentralizada, formada por la conexión directa de millones de computadoras u ordenadores mediante un protocolo especial de comunicación.

38. **Intranet**: Red interna de una organización diseñada y desarrollada siguiendo los protocolos propios de Internet.

39. **Licencia**: Es un contrato entre el autor del programa y el usuario que le permite al adquirente de la licencia utilizar el programa de forma legal. La licencia será adquirida, registrada y controlada por el funcionario a cargo del Área de Sistemas de Información o un representante autorizado.

40. **Lista de correo electrónicos**: Lista que contiene las direcciones de correo electrónicos de todos los usuarios que trabajan para la OCIF y que tienen acceso al correo electrónico.

41. **Medida o acción disciplinaria**: Sanción que se aplica a un funcionario o empleado que infringe las normas de conducta establecidas por perjudicar los mejores intereses de la OCIF o violentar los estatutos establecidos en este **Reglamento**.

42. **Nombre de Usuario o "Username"**: Nombre único en la red para tener acceso a un sistema computadorizado.

43. **OCIF**: La Oficina del Comisionado de Instituciones Financieras.

44. **Página de Internet**: Es una página que compone un sitio dentro de la World Wide Web (www).

45. **Periféricos**: Conjunto de partes o unidades electrónicas externas que se conectan externamente a un puerto de la computadora para ampliar sus funciones, tales como, impresoras, "scanners", mouse, teclado, proyector, o "drives".

46. **Privilegios de Acceso**: Nivel de Acceso que tiene un usuario para ver, modificar, borrar, copiar directorios y archivos o ejecutar programas dentro de un servidor. Estos privilegios se establecen dependiendo del trabajo que vaya a realizar un usuario dentro de una aplicación en específico.

47. **Programa ("software")**: Se refiere al conjunto de instrucciones que permiten que una computadora lleve a cabo su función. Puede haber programas que controlan el funcionamiento de las computadoras, de las redes de informática, y programas de aplicación que facilitan o automatizan las operaciones de una entidad para que no tengan que ser llevadas a cabo de forma manual.

48. **Programa Espía:** Programa que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

49. **Programa pirateado**: Programa que se instala o se copia sin la debida autorización de la compañía dueña del producto.

50. **Protocolo**: Lenguaje que utilizan dos computadoras para comunicarse entre sí.

51. "PST": Un archivo personal de correo electrónico en la aplicación "MS Outlook". Tiene una capacidad máxima de 2Gb y se guarda en la memoria de la computadora ("C") o en un dispositivo de memoria externo, como un disco duro o un "flash drive".

52. **Receptor erróneo o envío a dirección equivocada**: envío a una persona distinta de aquella a quien se intenta, ya sea por error del usuario o por interceptación de las líneas de comunicación o de los sistemas

53. **Red**: Sistema de telecomunicación para transferencia de datos que se conectan entre sí de manera interna o externa a los sistemas de información. Conjunto de equipos y programas electrónicos interconectados por varios tipos de dispositivos de telecomunicaciones como "LAC", "Networks", "Internet", "Telerate", "Bloomberg", y "CRD".

54. **Repositorio**: Local físico o virtual centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.

55. **Resguardo ("Back-up")**: Mecanismo para salvaguardar información copiando los archivos, datos o datos magnéticos, a un segundo medio (disco, cartucho removible) como precaución con el fin de que estén disponibles en caso de que un fallo produzca la pérdida de los archivos originales. Dicha información se reproduce individualmente por los usuarios o generalmente en un local físico o virtual centralizado y fuera de la OCIF donde se almacena y mantiene la misma de manera que se pueda recuperar la mayor cantidad de datos en caso de pérdida o desastre ("Disaster Recovery Back Up").

56. **Servidor o "server"**: Equipo de computadora ("file servers") con un sistema operativo que maneja los recursos de la red en una red y es capaz de proveer servicio a múltiples estaciones de trabajo.

57. **Sistema**: Acervo de programas, equipo y periféricos que conjuntamente con el usuario y los recursos disponibles tienen el propósito de satisfacer determinadas necesidades y resolver problemas en determinado ambiente.

58. **Sistema de Información o Informática**: Se refiere al uso y manejo de todo aquel equipo, aplicación, programa o periféricos utilizados para procesar información y para llevar a cabo las operaciones de la OCIF.

59. **Usuario**: Empleado de la OCIF o personal autorizado al uso de Sistemas de Información.

60. **Virus o contaminante**: Programa de computadora creado con el propósito de hacer daño al equipo, aplicaciones o información donde se instala.

61. **WWW ("World Wide Web")**: Es parte de la Internet, provee a las organizaciones o individuos una manera de publicar información a nivel mundial.

ARTÍCULO 6. Disposiciones Generales

La OCIF cuenta con acceso a computadoras, redes, servicios electrónicos internos y externos y la red de Internet. Al hacer uso de los equipos y servicios asociados, todos los usuarios acatarán las normas contenidas en este **Reglamento**.

1. Los equipos, los servicios asociados tanto internos como externos, el sistema de correo electrónico , sistema de facsímile, la Internet y los documentos y programas que se transportan por las mismas son propiedad de la OCIF y solo podrán ser

utilizados para propósitos lícitos, prudentes, responsables y dentro de las funciones inherentes de la OCIF.

2. El Comisionado, el Subcomisionado y los Comisionados Auxiliares o Directores de la OCIF tendrán la obligación de conocer, dar a conocer y mantener accesible a sus empleados una copia de este **Reglamento** en sus respectivas oficinas, de manera que el usuario de cada estación de trabajo conozca y cumpla rigurosamente con las disposiciones del mismo. El Comisionado, Subcomisionado, Comisionados Auxiliares, Asesor Legal General y todo su personal gerencial promoverán el buen uso y manejo de la información, así como el cumplimiento de los controles establecidos y de las políticas sobre seguridad de información. Cualquier acto que violente o intente violentar las disposiciones que mediante este **Reglamento** se promulgan, será investigado por un equipo de trabajo nombrado por el Comisionado.

3. Será requisito de todo usuario, para el uso y control de los Sistemas de Información, completar y firmar el documento **Acuse de Recibo del Reglamento para el Uso y Control de las Computadoras y Sistemas de Información** (Anexo I), en el cual se expresa el acuerdo del empleado en cuanto a la política de uso de esa herramienta de trabajo. El Área de Sistemas de Información será responsable de retener el original de dicho "Acuse de Recibo" firmado por el usuario y enviar una copia al Área de Recursos Humanos, para incluirse en el expediente del empleado.

4. El Área de Sistemas de Información será responsable de crear y publicar una página en Internet con información oficial de la OCIF.

5. Toda información, dato, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier derecho que surja, se cree o modifique mediante el uso de algún equipo de la OCIF será propiedad de la agencia, aunque la información, dato, escrito, documento, programa, acción privilegio, patente, derecho de auto o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario. La OCIF retiene el derecho de autor de cualquier material autorizado colocado en cualquier foro o página de Internet que fuere realizado por sus empleados en horas de trabajo y con equipo de la Agencia.

6. La información contenida en la computadora, los servicios asociados tanto internos como externos, los mensajes de correo electrónico, información de la Internet o la Intranet y los documentos y programas existentes no podrán ser reproducidos o utilizados para fines ajenos a las funciones y poderes de la OCIF. Cualquiera de esta información podrá ser examinada o utilizada por el Comisionado, el Área de Sistemas de Información o el Comité de Tecnología.

7. Se prohíbe el uso del equipo para enviar, recibir o crear mensajes o documentos de contenido discriminatorio por razones de raza, género, credo, ideas políticas,

orientación sexual, identidad de género, origen social o nacional, o que puedan ser catalogados como hostigamiento sexual. Se prohíbe además, la divulgación por cualquier equipo de cualquier tipo de opinión personal 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.

8. Al finalizar el día, los usuarios deberán retirar sus claves de acceso de los terminales y deberán apagar todos los equipos electrónicos en su área de trabajo, excepto por instrucciones al contrario. En caso de situaciones de emergencia tales como: huracán, tormenta, inundaciones, o averías a la planta física, los usuarios serán responsables de tomar las medidas necesarias y de cumplir con el Plan Operacional de Emergencias emitido por la OCIF para proteger el equipo bajo su custodia.

9. Aquellos usuarios que violenten de alguna manera lo dispuesto en este **Reglamento** podrán ser sometidas a acciones o medidas disciplinarias de acuerdo a la importancia y gravedad de la falta incurrida y la frecuencia de reincidencia en la infracción conforme establecido en el Reglamento sobre "NORMAS Y PROCEDIMIENTOS SOBRE MEDIDAS CORRECTIVAS Y ACCIONES DISCIPLINARIAS" (Orden Administrativa 2-87 "Normas y Procedimientos sobre Medidas Correctivas) según enmendado, toda vez que el no cumplir con las referidas normas constituye un uso indebido del equipo y los programas.

10. El hecho de que una conducta o actuación relacionada con las computadoras, redes, sistemas y recursos electrónicos de la OCIF no esté contemplada en estas advertencias y condiciones de uso de las computadoras, no impide que el usuario pueda ser sancionado, si a juicio del Comisionado se trata de una conducta o actuación imprudente o irresponsable en relación a los referidos equipos y recursos electrónicos. A los fines de estas advertencias 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 OCIF. 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.

11. Será responsabilidad de cada usuario utilizar la información contenida en sus sistemas de archivo electrónicos con el sólo propósito de realizar operaciones propias del servicio público y brindar un servicio de excelencia y calidad.

12. El Área de Sistemas de Información o el Comité de Tecnología será responsable de mantener al día las normas establecidas en este **Reglamento.**

ARTÍCULO 7. Comité de Tecnología

Para atender todos los reclamos de los usuarios en los momentos en que no exista personal suficiente en el Área de Sistemas de Información que pueda atenderlos y con la intención de que las áreas de la Agencia estén representadas y que cada una de ellas pueda aportar de manera efectiva a nuestro plan de mecanización y mejoras a los sistemas ya establecidos, se crea y se le da carácter de permanencia el Comité de Tecnología de la OCIF. Además, si en algún momento hiciera falta porque el personal del Área de Sistemas no estuviera disponible, el Comité de Tecnología coordinará las funciones que sean necesarias para la continuidad de los servicios y labores de la OCIF.

El Comité tendrá el deber de coordinar la colaboración de nuestros recursos internos y externos para obtener una visión completa de las necesidades a corto y a largo plazo en el campo de los Sistemas de Información. Esto con el propósito de:

1. Aumentar la efectividad y uniformidad en nuestros procesos y servicios, internos y externos, para cumplir y proveer un mejor servicio a nuestra ciudadanía así como honrar nuestros mandatos de Ley.

2. Mejorar la productividad en los procesos administrativos y operacionales.

3. Obtener el máximo de los equipos y programas electrónicos adquiridos.

4. Determinar las necesidades de adiestramiento en sistemas y coordinar con la División de Recursos Humanos la celebración de los mismos.

5. Reducir costos.

El Comité estará integrado por los miembros que determine el Comisionado, uno de los miembros deberá ser designado Presidente. El Comité podrá recibir la colaboración de un consultor externo. Los miembros del Comité, en consenso, elegirán un secretario que estará a cargo de levantar las minutas de la reunión y circularlas no más tarde de una semana de celebrada la misma.

El Comité en pleno se reunirá a discreción de sus miembros quienes coordinarán la fecha en la que todos estén disponibles. Las reuniones se conducirán por el Presidente de acuerdo a una agenda establecida. Para propósitos de coordinación el Presidente será responsable de que se notifique a los miembros y a cualquier otra persona invitada sobre la fecha de las reuniones ordinarias y extraordinarias, así como de la cancelación o posposición de tales reuniones. Toda notificación especificará la fecha, lugar y hora de las reuniones.

El Comité tendrá la responsabilidad de:

1. Revisar la sección del Plan Estratégico relacionado con los Sistemas de Información y este **Reglamento** para ofrecer recomendaciones.

2. Recomendar al Comisionado proyectos de mejoras a los sistemas de información.

3. Conocer los procesos de la implantación de los distintos proyectos del Plan Estratégico y de este **Reglamento** para asegurar que cumplan con las necesidades de los usuarios.

4. Revisar y recomendar, en cuanto a los sistemas de información, la política externa que garantice el buen uso, manejo y conservación del equipo y sus programas.

5. Sugerir las medidas correctivas necesarias en los casos en que ocurra algún incumplimiento a las disposiciones de este Reglamento.

6. Conocer que se prepare un programa de mantenimiento periódico a los sistemas y que se está cumpliendo con el mismo.

7. Verificar que existe para los empleados un plan de adiestramiento en sistemas y que se cumple con el mismo.

El Comité someterá al Comisionado los Informes de Progreso conforme a las metas establecidas en el Plan Estratégico y este **Reglamento**; Copia de la Minuta de cada reunión y cualquier otro asunto que le sea requerido.

ARTÍCULO 8. Disposiciones para la Adquisición e Instalación de Equipo

A. Adquisición de Equipo y Programas

1. El Comisionado proveerá los equipos electrónicos para facilitar y agilizar el flujo de tareas. El usuario utilizará estos equipos adecuadamente y tomará los cuidados necesarios para protegerlos y mantenerlos funcionando en óptimas condiciones de manera que se eviten daños y averías ocasionadas por accidentes o mal uso.

2. El Área de Sistemas de Información o el Comité de Tecnología será responsable de administrar, planificar y coordinar la automatización de las operaciones de la OCIF. Por lo cual será responsable de asesorar a todos los niveles sobre la adquisición de equipo como parte del desarrollo e implantación de sistemas de información. Además, será responsable de ofrecer apoyo técnico a través de su personal por medio de la correspondiente solicitud.

3. El Área de Sistemas de Información o el Comité de Tecnología será responsable de cumplir con las normas establecidas en el Reglamento Núm. 3381 conocido

como "Reglamento de Adquisición", de 2 de diciembre de 1986, según enmendado, que regula la adquisición de bienes y servicios no profesionales por la Rama Ejecutiva.

4. El Área de Sistemas de Información o el Comité de Tecnología será responsable de establecer los criterios y estándares a ser aplicados a la OCIF en cuanto a la cantidad y naturaleza del equipo a utilizarse. Así mismo, determinará la mejor instalación, configuración del equipo y sistemas operativos a adquirirse y a utilizarse.

5. Los Comisionados Auxiliares o Directores de cada Área de la Agencia deberán someter documentos al Área de Sistemas de Información o su representante autorizado para solicitar aprobación previo a cualquier remodelación de área y/o cualquier movimiento de cubículo para asegurarse de que el sistema tenga la capacidad en la red para los cambios sugeridos, que se tenga el material disponible para los cambios y que se cumpla con los estándares establecidos.

6. Toda solicitud de equipo, aplicación y licencia se hará a través del Área de Sistemas de Información o su representante autorizado quienes serán responsables de la adquisición, registro, asignación e instalación programas o aplicaciones que se mantendrán actualizadas en todo momento. La adquisición de computadoras, periféricos y programas requerirá la recomendación y aprobación del Área de Sistemas de Información o el Comité de Tecnología a fin de que se cumpla con los estándares establecidos en la OCIF y se provean las condiciones de trabajo más adecuadas al usuario. Además, verificarán que el equipo y los programas que se interesa adquirir cumplen con los requerimientos y necesidades del usuario establecidos por la OCIF.

7. Se prohíbe instalar programas en las computadoras que no hayan sido adquiridos por la OCIF o sin la autorización previa del Área de Sistemas de Información.

8. Tanto el equipo como los programas que adquieran las diferentes unidades administrativas serán sufragados con los fondos de la partida presupuestaria que se haya separado para estos fines. El Director o Comisionado Auxiliar de cada área deberá justificar por escrito la necesidad de adquirir el equipo o programas que solicite.

9. Podrán adquirirse, por vía de excepción, programas diferentes a los estándares de la OCIF cuando se determine que los mismos son necesarios en áreas de trabajo altamente técnicas e indispensables para lograr los requerimientos del usuario en beneficio de la OCIF. El Área de Sistemas de Información ofrecerá el asesoramiento técnico, recomendación y aprobación sobre los programas que

podrán adquirirse.

10. La acción de contratar cualesquiera servicios de consultoría en el ámbito descrito en este **Reglamento**, podrá requerir la participación del funcionario designado por el Comisionado o un representante autorizado. El Área de Sistemas de Información o el Comité de Tecnología será el responsable de coordinar y asesorar sobre la contratación de servicios de consultoría relacionados al uso y funcionamiento de los sistemas de información de la OCIF.

11. Cualquier consultor que sea contratado para que desarrolle un programa o aplicativo para la OCIF deberá adiestrar al personal de la Agencia sobre la manera en que fue realizado, entregar toda la documentación, los programas fuente ("Source Code") y toda aquella información que necesitase el personal de la OCIF para dar mantenimiento y/o arreglar el mismo.

12. El Comisionado utilizará productos "enlatados" ("software") en las distintas áreas de trabajo solamente si estos han sido legalmente adquiridos, si las licencias para su uso están vigentes y si la utilización de éstos es para mejorar la realización de las tareas de la agencia. La utilización de productos enlatados debe responder a los acuerdos establecidos en los contratos de utilización que la OCIF negoció al momento de la compra. Ningún usuario deberá utilizar en los sistemas de la OCIF productos enlatados que no estén respaldados por un contrato de utilización adquirido por la agencia.

B. Recibo e Inventario de Equipos

1. Cuando se reciban equipos o programas de una firma suplidora, el personal del Área de Sistemas de Información será responsable de abrir e inspeccionar el empaque en un término que no excederá de cinco (5) días laborables desde la fecha de entrega. El personal se asegurará de que los bienes recibidos sean los que, en efecto, fueron solicitados. Deberá cotejarse que todo programa o aplicación incluya la licencia previa a su instalación o de lo contrario, no podrán ser instalados y el número de propiedad que asignará el Encargado de la Propiedad de la OCIF.

2. Se prohíbe el uso de programas o recursos para los cuales no exista una licencia o autorización de uso válida a nombre de la OCIF. El Área de Sistemas de Información o el Comité de Tecnología velará por el licenciamiento de los productos y registrará las licencias en sus respectivas compañías.

3. El Área de Sistemas de Información será responsable de preparar y mantener un inventario del equipo y las aplicaciones propiedad en la OCIF, como medida de control de sistemas así como del lugar donde se encuentra el mismo y la

asignación de los mismos a los usuarios. Esto no sustituye las disposiciones del Reglamento Núm. 11 "Reglamento de Activo Fijo", del Departamento de Hacienda.

4. Anualmente el Área de Sistemas de Información preparará un inventario de Licencias. Se asegurará de que el trámite de registro de las licencias no exceda de diez (10) días laborables desde su fecha de recibo.

5. Las computadoras así como los equipos, accesorios, aplicaciones y programas se utilizarán para asuntos oficiales exclusivamente. No se permitirá el uso de éstos para asuntos no oficiales ni el almacenamiento de documentos no oficiales o personales en el referido equipo.

6. Todo equipo de computadoras, periféricos y telecomunicaciones pertenece a la OCIF y al Estado Libre Asociado de Puerto Rico por lo que deben ser utilizados única y exclusivamente para propósitos oficiales. La utilización de los equipos para la transmisión de datos, no deberán representar conflicto de intereses para los usuarios de los mismos. Toda transmisión de información deberá corresponder siempre a los mejores intereses de la OCIF. Se prohíbe el uso de los sistemas de información y comunicaciones de la OCIF para asuntos no oficiales, propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario, para el recibo y envío de mensajes en cadena, para tener acceso a compras, juegos, concursos, eventos, páginas de entretenimiento o cualquier otro asunto o servicio no oficial o ajeno a las funciones de la OCIF. Se prohíbe el almacenamiento de documentos no oficiales o personales en el referido equipo.

C. Instalación de Equipo

1. El Área de Sistemas de Información o su representante autorizado será responsable de asignar, instalar y configurar el equipo de las respectivas áreas. La instalación de cualquier equipo, periféricos y/o aplicaciones se hará únicamente por el personal autorizado del Área de Sistemas de Información. Asimismo, la instalación de aplicaciones desarrolladas internamente se hará por el personal designado del Área de Sistemas de Información.

2. El Área de Sistemas de Información asignará las computadoras personales o portátiles a aquellos usuarios que necesiten esta herramienta para desempeñar sus funciones. Conforme a ello, se reservan el derecho de intercambiar las computadoras y periféricos, según las necesidades de la OCIF.

3. Todo sistema de información adquirido por la OCIF se instalará y configurará con sus respectivos equipos, aplicaciones, periféricos y programas por personal diestro y designado para estas tareas. Ningún usuario deberá realizar tareas de

instalación de programas o accesorios por sí solo.

4. El Área solicitante será responsable de coordinar la fecha de instalación con el Área de Sistemas de Información. El empaque se mantendrá cerrado hasta tanto el personal técnico autorizado lleve a cabo la instalación. El equipo asignado será entregado a los usuarios quienes estarán obligados a cumplimentar el formulario "Recibo por Propiedad en Uso" y entregarlo al Encargado de la Propiedad. Será responsabilidad exclusiva del usuario a quien se le asigne el equipo, la custodia y seguridad del mismo en todo momento, incluyendo cuando ocurran notificaciones de posibilidad de desastres naturales.

5. Cualquier movimiento físico del equipo será informado y coordinado con el Área de Sistemas de Información y no se puede hacer sin la debida autorización del Director del Área de Sistemas de Información, o un representante autorizado. El Área de Sistemas de Información adiestrará a una o dos personas en cada Área para que en casos de emergencia, puedan desinstalar el equipo.

6. En ninguna circunstancia se instalará en las computadoras aplicaciones pre-programadas que no tengan la debida licencia adquirida por la OCIF. El Área de Sistemas de Información o el Comité de Tecnología tendrá la facultad de eliminar cualquier aplicación instalada que no cumpla con este requisito.

7. La instalación y el uso de aplicaciones comerciales que no hayan sido adquiridas por la OCIF, sino por un usuario de la Agencia, podrán autorizarse únicamente en los casos en que se determine que éstas contribuyen de manera esencial a la ejecución de las funciones del usuario de la estación de computadora y éste tenga consigo la licencia y/o autorización del fabricante para su uso. Esta disposición aplicará en áreas de trabajo altamente técnicas y especializadas, en las que el uso de dicho programa es indispensable para lograr los requerimientos del usuario en beneficio de la OCIF.

8. Conforme al inciso anterior el dueño del programa deberá entregar el mismo, la licencia y la documentación al Área de Sistemas de Información. Este se guardará hasta que el mismo deje de ser usado en cuyo caso se desinstalará y se devolverá toda la documentación al dueño.

9. Todo programa, aplicación o sistema de información desarrollado, preparado o confeccionado por un empleado o contratista de la OCIF para llevar a cabo sus funciones se considerará como propiedad exclusiva de la OCIF y deberá contar con la autorización del Área de Sistemas de Información. Por lo cual el empleado o contratista entregará el programa y toda la instalación, documentos correspondientes a la misma y cualquier otra información para la operación del mismo una vez sea instalado y aprobado por el Área de Sistemas de Información

o el Comité de Tecnología.

D. Seguridad del Equipo

1. Todo usuario de una estación de computadora será responsable del uso adecuado del equipo a su cargo y velará por su buen funcionamiento. Esto incluye estar atento a cualquier mal funcionamiento o indicio de problemas en la operación de la referida estación, en cuyo caso deberá notificar de inmediato, mediante llamada telefónica o correo electrónico al Área de Sistemas de Información, o un representante autorizado para que estos revisen, corrijan la falla, o de ser necesario, para que de inmediato ordene la reparación de los mismos. El uso inadecuado o mal uso del equipo asignado podrá conllevar la imposición de medidas disciplinarias.

2. Por razones de seguridad y protección del equipo, ningún usuario podrá:

    a. Ingerir alimentos cerca del equipo, o no tomar las debidas precauciones para evitar que en tales circunstancias se dañe el equipo; en caso de que ocurra un incidente que afecte el equipo por descuido, el usuario será responsable por cualquier daño que cause al mismo;

    b. permitir el uso del equipo por personas no autorizadas ajenas a la unidad organizacional o a la OCIF, exceptuando al personal externo debidamente autorizado para diagnosticar fallas de funcionamiento y la reparación o servicio del mismo;

    c. utilizar programas no relacionados con las funciones oficiales de la OCIF, como juegos u otros de similar contexto;

    d. utilizar programas de origen desconocido, ilegal u otros provistos por personas ajenas a la OCIF, sin el consentimiento de ésta. Lo anterior incluye programas de demostración que no hayan sido solicitadas a un suplidor reconocido;

    e. reparar los equipos, excepto que reciba instrucciones de así hacerlo y de cómo hacerlo por parte del Área de Sistemas de Información; y

    f. otras conductas de este tipo que pongan en riesgo el buen funcionamiento del equipo.

3. El Comisionado Auxiliar o Director del Área a la que pertenezca el equipo será responsable de que se cumpla cabalmente con esta norma. El uso inadecuado o

mal uso del equipo asignado a su personal podrá conllevar la imposición de responsabilidad al Comisionado Auxiliar o Director del Área si se demuestra que ello es consecuencia de no haber ejercido su deber de supervisión o no haber tomado las debidas precauciones con el personal a su cargo.

4. El Área de Sistemas de Información junto al Encargado de la Propiedad o un personal autorizado, autorizará la transferencia o préstamos de equipo a otros usuarios.

5. Aquellos usuarios a quienes se le asignen unidades portátiles son responsables de cuidar y proteger las mismas de daños físicos, accidentes o hurtos. Además, deben ser resguardadas para evitar la exposición al calor, exposición directa al sol y la humedad por tiempo prolongado. Las computadoras portátiles no pueden ser dejadas en los vehículos ni siquiera de manera oculta.

6. Los sistemas activarán automáticamente el protector de pantalla establecido para bloquear el acceso a esa computadora, cuando no se detecta actividad en la computadora.

7. Todo empleado que renuncie o sea separado de su puesto o se ausente por un lapso de tiempo prolongado ya sea por vacaciones, enfermedad o cualquier tipo de licencia, deberá hacer entrega a su supervisor, Director o Comisionado Auxiliar, del equipo que tiene en su estación de trabajo, incluyendo computadoras e impresoras portátiles, memorias removibles, llaves, documentos o cualquier otro material relacionado al equipo que está bajo su custodia, así como también la clave de acceso en caso de que sea necesario.

8. No se liquidará el pago final al empleado que cese en sus funciones hasta tanto se haya recibido el equipo, libros y documentos bajo su custodia.

ARTÍCULO 9. Clave, contraseña o "password" de acceso

1. Los accesos a cada sistema son otorgados al usuario, de acuerdo a las funciones que le han sido asignadas. El Área de Recursos Humanos, previa coordinación con el Comisionado Auxiliar, Director o supervisor del empleado solicitante notificará a Sistemas de Información los accesos requeridos para cada empleado a través del proceso determinado para ello que está contenido en la "Política y Procedimientos de Seguridad de Informática de la Oficina del Comisionado de Instituciones Financieras". La solicitud deberá indicar el nivel de acceso para llevar a cabo las funciones del empleado.

2. El Área de Sistemas de Información sólo le otorgará acceso a un empleado de acuerdo a lo que el supervisor, Director de Área o Comisionado Auxiliar de éste

solicitó conforme a las funciones del empleado solicitante y las que el dueño del módulo autorizó. Será responsabilidad del Director o Comisionado Auxiliar el uso que le dé a los sistemas de información el empleado bajo su supervisión.

3. Se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos sin la debida autorización de los custodios de la información concerniente.

4. Se prohíbe modificar los parámetros y configuración adoptada por la OCIF en las computadoras en la capacidad de recibir llamadas telefónicas, conexión remota o cualquier otro tipo de acceso no autorizado en la red. Esto incluye añadir, modificar o eliminar dispositivos periféricos, sonido, o apariencia de pantalla ("wallpaper" y/o "screen saver"), entre otros.

5. A todos los usuarios se les asignará una cuenta de acceso con un "username" que por lo general será el nombre del empleado con la inicial de su primer apellido. Si la cuenta del usuario permanece inactiva por un periodo mayor a noventa (90) días la misma será inactivada. Para lograr reactivar la cuenta nuevamente, el usuario deberá llenar el documento de acceso y entregarlo en el Área de Sistema de Información.

7. Pareada a esta cuenta de acceso a todo usuario se le asignará un código, clave, contraseña o "password" secreto la cuál será única e intransferible. Los usuarios serán responsables de salvaguardar las contraseñas de acceso a las computadoras y sistemas de la OCIF. Las contraseñas individuales no serán impresas, almacenadas y entregadas a otras personas.

8. El mínimo de cada "password" será de ocho (8) caracteres. Los "passwords" no deben ser nombres de personas conocidas, números en secuencia ni palabras comunes. Se recomienda la mezcla de caracteres alfanuméricos como letras, números o símbolos sin sentido gramático. Esta combinación debe ser de al menos una mezcla de tres (3) grupos de caracteres que mencionamos a continuación: letras mayúsculas, letras minúsculas, números y caracteres especiales. No deberá ser información con la cual se asocie a la persona, como por ejemplo la fecha de nacimiento, nombre del cónyuge o hijos, iniciales, etcétera.

9. Los "passwords" de los usuarios serán cambiados cada tres (3) meses. El sistema operativo de la red de información le pedirá automáticamente a cada usuario un "password" nuevo al vencerse el tiempo de expiración.

10. El usuario no deberá informar o dejar conocer su código de identidad ni su "password" a ninguna otra persona u usuario. Excepto circunstancias de

emergencia posteriormente justificadas por escrito, si por la naturaleza de sus funciones un usuario debe tener acceso a la cuenta de otro (Ej. Asistentes Administrativos), se les proveerá, previa solicitud aprobada, privilegios de visualizar y enviar "on behalf of". De sospechar que su contraseña ha sido revelada por inadvertencia o descuido, los empleados deberán notificar inmediatamente al Área de Sistemas de Información para tomar las medidas correspondientes de seguridad. Si por alguna emergencia o circunstancia excepcional se requiriera que un usuario utilice la clave propia de otro para realizar alguna transacción, deberá mediar una autorización por escrito del usuario dueño de la cuenta y esta autorización será guardada en el expediente del propietario de la cuenta. De no estar disponible el usuario propietario de la cuenta, deberá mediar una autorización del Comisionado para permitir el acceso a esta.

11. El usuario será responsable de cualquier transacción efectuada bajo su clave de acceso. El observar cualquier uso no autorizado deberá informarlo al Área de Sistemas de Información o el Comité de Tecnología inmediatamente.

12. El sistema bloqueará la cuenta ("account lock out") del usuario, si éste se equivoca tres (3) veces consecutivas al entrar su contraseña. Para reactivar su cuenta, el usuario deberá comunicarse con el Área de Sistemas de Información.

13. La información, trabajos y documentos elaborados a través de las computadoras no tendrán clave de acceso, a excepción de aquellos en que los niveles directivos de la unidad de trabajo lo determinen y autoricen. No se podrá archivar o modificar la información propiedad de la OCIF con el propósito de impedir que alguien pueda leerla, entenderla o utilizarla. Tampoco se podrá alterar el nombre del usuario u otra información que se utilice regularmente para identificar la información, mensajes o archivos. En caso de que algún usuario asigne contraseñas o cifre la información ("encrypt") con el fin de evitar que personas puedan leerla, éste proveerá todos los datos para lograr acceso a los archivos al momento de su creación. La OCIF está facultada para decodificar la misma o restituirla a su condición original.

14. En casos de ausencia prolongada el empleado se hará responsable de coordinar con su Comisionado Auxiliar, Director de Área o supervisor un "password" provisional para que éste tenga acceso a los datos o archivos que se requieran en caso que sea necesario acceder a esos archivos. En situaciones de extrema emergencia o ausente oficial, el Área de Sistemas de Información podrá hacer los trámites necesarios para el acceso al equipo. El Director de Oficina o de Área solicitará la petición por escrito al Área de Sistemas de Información.

15. El uso de un "password" no impedirá que se audite el sistema y no significa que

el usuario albergue expectativa de intimidad alguna con relación a la información almacenada en la computadora que tenga asignada o en cualquier otra.

16. El Director del Área de Sistemas de Información o el Comité de Tecnología tiene la autoridad para delegar en algún empleado del Área el que pueda acceder a cualquier computadora para auditarla.

17. Durante el curso de una investigación de conducta impropia o de violación de Ley, Procedimientos o de Reglamentos, la OCIF puede acceder mensajes de correo electrónico, con o sin previo aviso al usuario. Será necesaria la autorización de cualquiera de los siguientes oficiales: (a) el Comisionado de Instituciones Financieras o el Subcomisionado y (b) el Comisionado Auxiliar de Administración o el Director de Recursos Humanos.

18. En relación con el inciso anterior, el Área de Sistemas de Información, o un representante autorizado deberá enviar un mensaje al usuario para que proceda a cambiar la contraseña de acceso, cuando regrese al trabajo.

19. Cualquier acceso a una base de datos se concederá de acuerdo a las funciones del empleado solicitante.

20. El Área de Recursos Humanos tiene la responsabilidad de notificar al Área de Sistemas de Información cuando un empleado ha renunciado, ha sido despedido, transferido a otra área, promovido, o ha cambiado de funciones para removerle los privilegios de acceso o hacer cambios a los mismos, el mismo día de la renuncia, despido, transferencia o promoción. Esta notificación se hará de acuerdo al procedimiento establecido en las Políticas y Procedimientos de Seguridad de Informática de la Oficina del Comisionado de Instituciones Financieras".

21. El Área de Sistemas de Información o el Comité de Tecnología será responsable de inactivar la cuenta del empleado inmediatamente cuando éste cese sus funciones en la OCIF y transcurrido dos (2) meses calendario se eliminará la cuenta y toda información irrelevante. Solo se mantendrá la información necesaria para el funcionamiento y mantenimiento de las operaciones de la OCIF.

ARTÍCULO 10. Uso del Internet

1. Internet es un recurso que la OCIF da a sus usuarios para realizar las funciones de sus puestos. El Internet es un privilegio y bajo ningún concepto puede ser interpretado como un derecho. Sin embargo, el uso personal ocasional de este recurso es permitido, en tanto no interfiera con la productividad del personal y

así haya sido autorizado por su Comisionado Auxiliar, Director de Área o supervisor y no cause conflictos con la actividad de la OCIF. Toda información transmitida por este medio será tratada como información relacionada con la OCIF y debe estar alineada a las normas enumeradas en este **Reglamento.** Ningún empleado autorizado a usar Internet podrá reclamar interés propietario o tener expectativa razonable de intimidad sobre comunicaciones utilizando dicho medio. La OCIF tendrá acceso a los mensajes electrónicos e información de los espacios virtuales (Web) visitados por empleados en cualquier momento y los mismos serán considerados parte de los expedientes de la OCIF.

2. Los medios de redes de comunicación y computadoras personales para acceso a los servicios de Internet se proveen a todos los usuarios. La OCIF monitorea todos los accesos a la Internet, por lo tanto esta herramienta deberá ser utilizada moderadamente. La OCIF se reserva el derecho de monitorear, auditar y restringir o bloquear el uso del Internet según sea necesario para cumplir con los términos aquí dispuestos y para asegurar el mejor funcionamiento de la red de comunicaciones. El Área de Sistemas de Información configurará un registro para los sitios Web visitados y los archivos descargados para monitorear las actividades. Este monitoreo puede ser mediante el uso de un sistema computadorizado a esos efectos o mediante verificación visual del registro en cada computadora.

3. Las políticas de Internet serán revisadas periódicamente en caso de que surjan nuevas necesidades, únicas y particulares a la OCIF. Se incorporan y se hacen formar parte de estas advertencias todos los documentos, memorandos, instrucciones, manuales o políticas que se notifiquen de tiempo en tiempo y que sean pertinentes al uso de las computadoras en la OCIF.

4. El usuario no podrá dejar su navegador abierto cuando no esté utilizando la Internet. Tendrá que cerrar la sesión para evitar el consumo de ancho de banda innecesario y que cualquier persona no autorizada la accede.

5. La OCIF podrá proveer acceso inalámbrico a una red donde sea viable, sea segura y garantice la integridad de las redes, sistemas, aplicaciones y datos mediante la implantación de técnicas de segmentación y autenticación. Dicho acceso solo se otorgará a aquellos empleados cuyas funciones de trabajo así lo requieran.

6. Los usuarios con necesidades de acceso remoto, empleados o contratistas, tienen que ser autorizados adecuadamente por el Área de Sistemas de Información.

7. Todo usuario es responsable por sus acciones y conducta al acceder el Internet. Siempre debe tener presente que la Internet es un conjunto de redes, por lo que su uso debe ser correcto y conforme a las políticas establecidas por los diferentes administradores de éstas. Bajo ninguna circunstancia los usuarios realizarán actos que puedan considerarse ilegal, inmoral, u ofensivos.

8. El acceso al Internet no podrá utilizarse en forma alguna, pero no limitado a:

   a. Procesar documentos, programas o información que pueda ser fraudulenta o catalogado como molestosos, embarazosos, indecentes, profanos, obscenos, intimidantes, ilegales o inmorales. Esto será así independientemente de que sean enviados o recibidos por correo electrónico o por cualquier otra forma de comunicación electrónica o de que sean presentados en pantalla o estén almacenados en computadoras de la OCIF.

   b. Acceder a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía. Se prohíbe archivar, almacenar, distribuir, editar, bajar de Internet, reproducir o enseñar cualquier tipo de material o imagen sexualmente explícita utilizando la red de comunicaciones del área de trabajo. Si usted por alguna razón se conecta accidentalmente a una pantalla con material sexualmente explícito, se deberá desconectar inmediatamente.

   c. Bajar o distribuir data o programas pirateados.

   d. Acceder a sitios Web relacionados con música, juegos, apuestas, videos, u otros sitios de entretenimientos on-line; Este tipo de contenido satura la Red y por ende requiere una mayor cantidad de recursos (ancho de banda) lo que afecta el funcionamiento de la misma.

   e. Acceder a sitios Web de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, bromas de mal gusto, prejuicios, menosprecio, o acoso explícito.

   f. Acceder a sitios de "hacking" o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información de la OCIF.

g. Descargar desde Internet cualquier material (incluyendo software) protegido bajo leyes de derecho de propiedad, o archivos electrónicos para usos no relacionados con la actividad de la OCIF. (Ej. Archivos de música o video).

h. Bajar información "download" de los servicios de Internet sin la debida autorización del Área de Sistemas de Información. Se exceptúa de esta prohibición al personal encargado de brindar mantenimiento a las computadoras, redes, servicios electrónicos y la red de Internet.

i. Publicar cualquier tipo de información perteneciente a la OCIF en sitios personales u otros, sin la autorización correspondiente del propietario de dicha información.

j. Publicar comentarios no profesionales en foros públicos, sitios de "chat", "Weblogs" (Blogs), correo electrónico, o cualquier otro medio de publicación en Internet.

k. Usar los programas de "chats", excepto sea autorizado por el Área de Sistemas de Información.

l. Participación en cualquier actividad ilegal o criminal.

m. Solicitud no autorizada de dinero o la operación de negocios personales.

n. Obtención de acceso no autorizado sobre otras computadoras pertenecientes a cualquier otra organización o entidad.

o. Instalación y uso de programas de tipo "peer-to-peer" para el intercambio de archivos en Internet (Ej. Kazaa, Morpheus, Limeware, etc.)

p. Instalación y uso de programas de "Instant Messenger" (Ej. Google Talk, Yahoo, AOL, Facebook Messenger, etc.)

q. Acceder a páginas de política partidista.

r. Incurrir en acoso cibernético o asecho cibernético contra cualquier empleado, contratista o cualquier otra persona de manera continua y sistemática. El así hacerlo se considerará una violación no solo a este

Reglamento sino al Reglamento de la OCIF para la Prevención y Sanción por Hostigamiento Sexual.

s. Amenazar, acosar, hacer declaraciones falsas o difamatorias sobre otros; enviar correo de odio, chistes o comentarios discriminatorios utilizando lenguaje que generalmente se considere ofensivo para las personas si es basado en raza, herencia étnica, origen nacional, sexo, orientación sexual, identidad de género, edad, físico o enfermedad mental o discapacidad, estado civil, religión u otras características que puedan estar protegidas por derechos civiles.

En caso de que algún usuario o área requiera el acceso a este tipo de sitios como parte de sus funciones laborales relacionadas con la OCIF, deberá previamente justificar por escrito la necesidad y obtener la autorización de la misma manera de su respectivo Comisionado Auxiliar, Director de Área o supervisor. En caso que el acceso a un sitio en particular esté deshabilitado deberá solicitar la apertura vía correo electrónico a help@ocif.gobierno.pr

ARTÍCULO 11. Uso del Correo Electrónico

Los sistemas de correo electrónico son propiedad de la OCIF y la información contenida en los mismos son récord de sus operaciones. El personal de la OCIF utilizará el correo electrónico exclusivamente para propósitos oficiales. Ningún empleado autorizado a usar esta herramienta podrá reclamar interés propietario o tener expectativa razonable de intimidad sobre comunicaciones utilizando dicho medio. La OCIF tendrá acceso a los mensajes electrónicos e información en cualquier momento y los mismos serán considerados parte de los expedientes de la OCIF.

1. Los usuarios de sistemas de correo electrónico tienen que estar conscientes de los riesgos implícitos en este medio de comunicación como la interceptación, supervisión pasiva, interceptación activa, autenticación, violación de confidencialidad, envío a receptor o dirección errónea.

2. Toda información contenida en el sistema de correo electrónico está clasificada como oficial. Como tal, la información que tiene que ser retenida para rastro de auditoría o que forma parte de un expediente o record permanente se debe mantener en un medio apropiado.

3. Todo mensaje por correo electrónico deberá tener como justificación el intercambio de información oficial relacionada con los deberes y funciones del empleado. Los mensajes de correo electrónico pueden ser considerados como evidencia legal. Cualquier mensaje que sea parte de una negociación, un contrato de servicio, asunto legal o de trabajo, se podría requerir como evidencia en corte, por lo que deberá ser guardado

cuidadosamente en un directorio que no sea borrado accidentalmente.

4. El Área de Sistemas de Información asignará el privilegio de enviar documentos a todos los usuarios de la red de manera restringida.

5. El sistema de correo electrónico no es el medio apropiado para transmitir información privada o confidencial. Los usuarios del sistema de correo electrónico deben asegurarse del estricto cumplimiento con las normas de confidencialidad de la OCIF sobre la divulgación de información. El Comisionado exige que toda información contenida en los sistemas de archivo electrónico, sin importar el medio en que se encuentre, no sea divulgada, salvo permitido por ley y previa autorización.

6. Todos los mensajes de correo electrónico llevarán escrito en la parte inferior del documento la advertencia de "Nota de confidencialidad" que protege los derechos de confidencialidad de la OCIF. Dicha advertencia incluirá un aviso para prevenir la distribución no permitida y que se remite "Para uso exclusivo del destinatario".

7. El usuario del sistema de correo electrónico reconoce que:

    a. Tiene que verificar el correo electrónico diariamente.

    b. Cualquier material escrito, preparado y enviado por correo electrónico interagencial deberá ser revisado por funcionarios autorizados.

    c. Los usuarios no podrán utilizar el correo electrónico para enviar a personas o entidades fuera de la OCIF documentos internos sin el previo consentimiento de quien originó el documento.

    d. Bajo ningún concepto un empleado podrá facilitar la información a terceras personas que no sea para realizar sus funciones como empleado del Estado Libre Asociado de Puerto Rico.

    e. El contenido de los mensajes personales no está protegido de manera alguna y la OCIF no tiene responsabilidad en caso de ser accedidos en el curso de asuntos oficiales de la OCIF o por terceras personas en cualquier momento o circunstancia.

    f. La OCIF no tiene la intención de intervenir los mensajes por correo electrónico rutinariamente. Sin embargo, de acuerdo con las normas de la Oficina, puede accederlos, con o sin previo aviso al usuario, por cualquier razón, incluyendo pero sin limitarse a propósitos oficiales, propósitos de mantenimiento de sistemas, o propósitos de investigación.

g. Los mensajes enviados a través de correo electrónico pueden ser desviados. Generalmente esto sucede por error del que envía, pero pueden suceder errores en los directorios del sistema o en la ruta de transmisión.

h. Los mensajes de correo electrónico re-dirigidos y sus anexos, no llegan siempre en la condición en que fueron recibidos o enviados.

i. Los mensajes de correo electrónico no llegan siempre a tiempo, por lo que el usuario que lo utilice para enviar una comunicación con un tiempo de cumplimiento debe asegurarse que el documento o comunicación llega al destinatario en el tiempo requerido.

j. Los archivos de correo electrónico son respaldados diaria, semanal y mensualmente y la OCIF mantiene un Plan de Continuidad de Negocios y Recuperación de Desastres. No obstante, los sistemas no son infalibles y aunque los respaldos diarios se guardan por lo menos cinco (5) días, los semanales por cinco (5) semanas y los mensuales durante doce (12) meses, los respaldos no son para proveer controles de auditoría de mensajes. Por tanto, el usuario es responsable de la preparación y mantenimiento de copias de mensajes y documentos que origina o transmite.

8. Para cumplir con requerimientos judiciales o de autoridades con facultad legal para obtener tal información, los mensajes o cualesquiera otros datos en el sistema de correo electrónico pueden ser accedidos con o sin previo aviso al usuario por terceras personas. Antes de proveer cualquier información, bajo un requerimiento judicial o de autoridad con facultad legal para solicitarla, será necesaria la aprobación de la División Legal de la OCIF.

9. En caso de ser necesario acceder mensajes de otro usuario para obtener información de sus operaciones oficiales, se requiere la autorización expresa del Comisionado o del Subcomisionado. La OCIF limitará al mínimo el acceder a los mensajes, tanto para el mantenimiento del sistema de correo electrónico, como para localizar y recobrar información necesaria. Sin embargo, algunos procedimientos de mantenimiento de sistemas requieren invadir los archivos de mensajes, por tanto el usuario es responsable de familiarizarse con el criterio de mantenimiento y ajustarse a los requisitos de éste.

10. Las cuentas de correo electrónico serán para propósitos de agilizar la distribución de información entre los empleados. Por tal razón, cada mensaje que escriba el usuario tiene que ser necesario, conciso y cortés. Los usuarios evitarán enviar mensajes que puedan ser fraudulentos o catalogados como difamatorios, molestosos, embarazosos, indecentes, profanos, obscenos, intimidantes, ilegales o inmorales.

11. Está expresamente prohibido:

a. El uso del sistema de correo electrónico para asuntos personales o no oficiales de la OCIF.

b. El divulgar información o documentos de la OCIF o de terceros a organizaciones o individuos externos sin autorización. Se prohíbe el envío o recibo de mensajes electrónicos entre el personal de la OCIF y otras personas ajenas al mismo en los cuales se divulguen, comenten o expresen hechos, opiniones u otras situaciones o asuntos internos de la OCIF que puedan poner en entredicho la reputación y la imagen de la Oficina.

c. El incluir material sensitivo relacionado con litigios en proceso o potenciales.

d. El hacer comentarios insultantes sobre productos o servicios de terceros, que puedan dar a entender que es la opinión de OCIF.

e. El utilizar material que pueda violentar derechos reservados o de autor.

f. Duplicar programas licenciados adquiridos por la OCIF o con derechos de autor a menos que se especifique explícitamente que está permitido. Está estrictamente prohibido la reproducción de cualquier "software" perteneciente a la agencia, bien sea que se haya adquirido o desarrollado internamente, para beneficio personal de cualquier usuario o de terceras personas, o con intención de afectar, de cualquier modo, los mejores interese de la agencia. La OCIF no requiere, solicita, ni condona la duplicación o uso no autorizado de programas protegidos por derechos de autor.

g. El realizar actividades contrarias o prohibidas en las Normas de Conducta de la OCIF.

h. El promover actividades políticas.

i. El suscribirse a listas de correo electrónico o que participen en grupos de noticias ("newsgroups") que divulguen información o mensajes ajenos a las funciones y deberes de la OCIF sin la debida autorización.

j. El acceder los archivos de correo electrónico o los recursos del sistema de un usuario sin justificación alguna o sin la autorización del personal designado.

k. Se prohíbe archivar, almacenar, distribuir, editar, recibir, enviar o enseñar cualquier tipo de material o imagen sexualmente explícito, obsceno, profano u ofensivo utilizando el correo electrónico. Esto incluye, a modo de ejemplo, acceso a material erótico, bromas de cualquier forma o cualquier comentario o

chiste que pueda violar la política anti discrimen y contra hostigamiento sexual en el empleo que prevalece en la OCIF.

l. La falsa representación del remitente de un mensaje con intención de engañar, accediendo sin autorización o utilizando los códigos de identificación de otra persona. Se prohíbe enviar mensajes a diferentes personas utilizando el correo de una tercera persona sin su debida autorización.

m. El uso negligente del correo electrónico que resulte en daños de cualquier naturaleza a la OCIF o a terceros.

n. El conducir operaciones o transacciones que impongan obligación legal mediante correo electrónico, excepto mediante el uso de medidas de seguridad autorizadas por la OCIF.

o. El uso del correo electrónico para informar, apercibir, presentar, dar seguimiento, discutir y/o dilucidar cualquier asunto sensitivo relacionado a la administración de los recursos humanos y/o transacciones de personal; para presentar, informar, dar seguimiento, discutir y/o dilucidar controversias entre compañeros y/o supervisores; para efectuar cualquier tipo de señalamientos, incluyendo, pero no limitado a, señalamientos éticos y/o criminales, en contra de otros compañeros y/o de la OCIF. Así las cosas, la naturaleza sensitiva e incluso confidencial de este tipo de asuntos requiere un grado de formalidad que no puede obtenerse mediante el envío de un correo electrónico. Por tanto, si algún empleado tiene una situación de la naturaleza previamente descrita y desea que su reclamo y/o consulta sea considerada deberá, sin excepción, seguir las canales de comunicación que en adelante se establecen:

    i. Establecer la situación por escrito mediante comunicación dirigida a su supervisor.

    ii. El supervisor dentro del término de cinco (5) días laborables suscribirá una comunicación dirigida al empleado informando su determinación (la cual puede incluir referir el asunto a la Oficina de Recursos Humanos).

    iii. Si el empleado no está de acuerdo con la determinación del supervisor, deberá dentro del término de cinco (5) días laborables a partir del recibo de dicha determinación, presentar el asunto por escrito ante la Oficina de Recursos Humanos para la acción correspondiente.

12. En la eventualidad de que el usuario vaya a ausentarse por un periodo de tiempo, será

su responsabilidad el coordinar el reenvío ("forwarding") automático temporero a una persona designada. Esto se hará mediante la herramienta de "Microsoft Outlook" en el "out of the office assistant", cuyo procedimiento se cubre en el adiestramiento a los usuarios de dicho programa.

13. El usuario que desee restaurar archivos de correo tendrá que justificarlo por escrito.

14. El usuario no podrá solicitar detener mensajes. Una vez remitido, el mismo no podrá ser recuperado, excepto mediante la función en Microsoft Outlook que provee el sistema de correo electrónico para el usuario.

15. Periódicamente, el usuario eliminará o archivará apropiadamente los mensajes que ya no son necesarios y que no vayan a ser utilizados posteriormente. Se dispondrá de la información que se almacena en medios magnéticos y cuyo periodo de utilización haya terminado, usando los procesos automatizados vigentes. El archivo de anexos de mensajes requiere de bastantes recursos del sistema. El usuario debe remover, por lo menos cada quince (15) días, los archivos, programas o anexos y archivarlos en un servidor de manera que se pueda utilizar al máximo el espacio en el disco de la computadora. Todo tipo de archivo o programa ajeno a las funciones y deberes de la OCIF deberá ser removido o eliminado de los equipos electrónicos inmediatamente se detecte la existencia del mismo.

16. Cada usuario será responsable de crear en su computadora un archivo de resguardo conocido como "PST" en el cual debe guardar aquellos correos que considere necesario conservar. Si los mensajes son parte de aplicaciones de producción o documentación de proyectos y tienen que ser almacenados para uso posterior o para record, se copiarán los mensajes fuera del sistema de correo electrónico en un sistema de almacenaje apropiado. El Área de Sistemas de Información asesorará al usuario sobre el proceso adecuado.

17. Antes de enviar archivos ejecutables por correo, asegurarse de que no está violando derechos de propiedad intelectual, derechos reservados o derechos de autor.

18. La descarga de programas no está permitida sin autorización previa y siempre que se cumplan las siguientes condiciones:

    a. la autenticidad del "software" está debidamente comprobada; han sido investigadas y determinadas las condiciones para su uso (incluyendo costos de "shareware"), y estas condiciones han sido cumplidas;

    b. que el programa se instale de acuerdo a las políticas de seguridad correspondientes;

c. el programa fue examinado por una versión actualizada del antivirus estándar de la OCIF.

19. Los archivos ejecutables recibidos a través de correo electrónico tienen que ser escrutados para virus antes de ser ejecutados. Es imprescindible copiar los archivos ejecutables en un disco y examinarlos con un programa antivirus previo a su ejecución. Los archivos comprimidos deben ser examinados antes y después de descomprimirlos.

20. Antes de separarse del empleo, el usuario removerá cualquier mensaje o archivo con información innecesaria, irrelevante o repetida.

21. Limitar el número y tamaño de los anexos enviados por correo electrónico. Enviar archivos muy grandes o mensajes que contengan muchos anexos puede afectar adversamente el desempeño del sistema de correo electrónico para todos los usuarios.

22. Ejercer cautela al dirigir mensajes para prevenir que sean enviados a receptores equivocados.

23. Nunca originar o retransmitir mensajes de los conocidos como "Mensajes en Cadena". De recibir alguno que contenga advertencias o sugerencias de cualquier naturaleza, remitirlo al Administrador del Sistema de Correo Electrónico para la acción correspondiente.

24. Los Comisionados Auxiliares o Directores de Área tendrán la responsabilidad de:

a. Supervisar y asegurar el estricto cumplimiento de los usuarios de su unidad con este **Reglamento.**

b. Asegurar que los privilegios de acceso se descontinúen apropiada e inmediatamente en casos de traslados, separaciones o cambios de asignación.

c. Asegurar la integridad y retención de los archivos de usuarios que han sido identificados por la Oficina del Contralor de Puerto Rico u otro oficial autorizado para su investigación.

d. Con la previa autorización del Comisionado o del Subcomisionado, coordinar la extracción de información oficial del archivo de correo electrónico de usuarios que cesan en sus funciones. Proveer al Administrador del Sistema de Correo Electrónico el nombre del usuario autorizado y el nombre del dueño del archivo en cuestión.

e. De ser posible, informar al usuario que su archivo de correo electrónico será intervenido para extraer información oficial. Cuando sea autorizado por el Comisionado o Subcomisionado, el Administrador del Sistema de Correo Electrónico permitirá al usuario autorizado acceder el archivo electrónico, remover información innecesaria, irrelevante o repetida.

25. El Administrador del Sistema de Correo Electrónico tendrá la responsabilidad de:

a. Asegurar la disponibilidad y confiabilidad del sistema de correo electrónico.

b. Asignar y dar soporte a la distribución de direcciones del sistema de correo electrónico.

c. Avisar a los usuarios sobre fallos en la entrega de mensajes y ayudar en su recuperación.

d. Administrar los recursos de archivo del sistema de correo electrónico provistos a los usuarios y cotejar su uso basado en las guías delineadas en la sección "Mantenimiento de Sistemas".

e. Permitir que se pueda acceder para lectura los archivos de correo electrónico de usuarios específicos a solicitud expresa de funcionarios facultados.

f. Retener durante tres (3) semanas los archivos de correo de los usuarios separados del empleo.

g. Revisar periódicamente el Plan de Continuidad de Negocios y Recuperación en caso de desastres de acuerdo con las normas de la OCIF.

h. Administrar el proceso de respaldo del Sistema de Correo Electrónico y de su base de datos.

i. Administrar la retención de los mensajes de correo electrónico de los usuarios de acuerdo a las mejores prácticas de retención de mensajes.

j. Proteger la integridad y custodiar los archivos de correo electrónico en cumplimiento con requerimientos judiciales.

ARTÍCULO 12. Normas para la protección antivirus

Es responsabilidad de los usuarios de la red de computadores de la OCIF aplicar todas las medidas preventivas disponibles para proteger los sistemas contra la infección por virus, "malware", "phishing", etc.

Estas normas describen cómo varias clases de virus pueden infectar la red de la OCIF, cómo el Área de Sistemas de Información o el Comité de Tecnología de OCIF intenta prevenir o reducir las incidencias de infección y cómo los usuarios de la red de computadoras de la OCIF deben reaccionar ante un virus cuando sospechan que esté infectada la red.

1. La mayor parte de los virus se transportan anexados a mensajes de correo electrónico. Los anexos pueden ser documentos de trabajo, presentaciones o bien pueden ser fotografías, bromas, dibujos animados, direcciones en la Web u otros. Tales anexos pueden ser remitidos con la intención de infectar la red de la OCIF o sin conocimiento de que están infectados, pues algunos virus al abrirse el anexo que los contiene automáticamente generan y remiten mensajes por correo electrónico contaminados sin que el remitente advenga en cuenta que su computadora está infectada.

2. Nunca abra archivos o macros recibidos en anexos a mensajes de correo electrónico recibidos de remitentes desconocidos, sospechosos o de procedencia no confiable. Estos anexos deben ser desechados inmediatamente y seguidamente se vaciará la carpeta de reciclaje para que no queden en la computadora.

3. Deseche de inmediato mensajes en "spam", en cadena o "junk", nunca los reenvíe.

4. Los virus pueden introducirse en la red y contaminarla propagándose mediante varias clases de medios de almacenaje. Como en el caso de los anexos de correo electrónico, los virus pueden esconderse en documentos de trabajo legítimos grabados en disquetes, discos CD, DVD, ZIP, "pen drives" u otros medios removibles o simplemente presentar esa apariencia.

5. El descargar programas a través de la red cibernética puede ser una fuente de infección. Como en otras transmisiones, los virus pueden esconderse junto a programas legítimos. Nunca intente descargar programática de origen desconocido o sospechoso.

6. Aunque menos comunes que anexos de correo electrónico, cada vez más virus se aprovechan de la programática de mensajería instantánea, que se usa para dar respuestas rutinarias automáticas, tal como acuses de recibo. Estos anexos operan igual que los de correo electrónico en la transportación de virus, pero por el servicio que presta la mensajería instantánea y provenir de una fuente confiable con la que se realizó una gestión, no levanta sospecha de origen.

7. El Área de Sistemas de Información de la OCIF combate los virus de varias maneras:

    a. Al comienzo de las operaciones diarias, cuando los usuarios activan las estaciones de trabajo, el programa antivirus de la estación hace conexión al Servidor Antivirus de la OCIF para actualizar automáticamente su propio archivo. El Área de Sistemas de Información opera dicho programa en todos los servidores y estaciones de trabajo para combatir los virus. Se escudriñan todos los datos que se graban o leen en el disco duro de la estación o en el que use la estación en la red. Además, verifica todo el tráfico en la red cibernética o enviado a ella. Solo se permite que el tráfico de clases específicas pase a través de los recursos de protección provistos. Por ejemplo, un mensaje de correo electrónico originado externamente tiene que pasar por el programa antes de aceptarla ese servidor. Este programa puede enviar el mensaje sospechoso y sus anexos a un área de almacenamiento aislada y tratará de remover el virus. De no lograrlo, lo desecha y envía un aviso al receptor de la incidencia y la acción tomada.

    b. Diariamente el Servidor Antivirus de la OCIF hace conexión al Servidor Antivirus de la Oficina de Gerencia y Presupuesto para actualizar el archivo de definiciones de virus. Estos archivos permiten que el programa pueda reconocer virus nuevos. De encontrar nuevas definiciones de virus, el archivo es actualizado automáticamente e informa al Área de Sistemas de Información.

8. Aunque todos los servidores en la red de computadores de la OCIF, así como todo el tráfico desde y hacia la red cibernética son escudriñados para la detección de virus, existe la posibilidad que un virus nuevo o uno muy escondido alcance a una estación de trabajo. Si el incidente no es atendido adecuadamente, el virus puede infectar la red de la OCIF.

9. El Área de Sistemas de Información o el Comité de Tecnología de la OCIF notificarán a todos los usuarios por correo electrónico o por teléfono en caso de que surja un riesgo inminente de infección por virus. Este aviso de infección por virus será a todos los usuarios, por lo que al recibirlo los usuarios no deberán reenviarlo. Ocasionalmente, personas actuando con buena intención remiten avisos falsos de virus. Estos avisos típicamente no son dañinos, sin embargo, reenviar estos mensajes incrementa innecesariamente el tráfico por las redes de comunicaciones.

10. Como indicado anteriormente, es responsabilidad de todos los usuarios de la red de computadoras de la OCIF dar los pasos necesarios para impedir la propagación de virus. Para contribuir en este esfuerzo, los usuarios:

a. No deberán acceder a anexos en mensajes de correo electrónico que no esperan, aunque sean de usuarios de la misma oficina si éstos le resultan sospechosos.

b. No deberán acceder anexos del mensaje de correo electrónico o de mensajería instantánea de un remitente desconocido o sospechoso sin la autorización del Área de Sistemas de Información.

c. Nunca deberán descargar programática desde la red cibernética sin la autorización del Área de Sistemas de Información.

d. De recibir un archivo que contiene macros y no hay seguridad de su procedencia, deberá ser inhabilitado. De necesitar habilitarlo, obtendrá la autorización del Área de Sistemas de Información.

e. En caso de recibir archivos o anexos en correos electrónicos sospechosos, pero interesan accederlos, deberán informarlo al Área de Sistemas de Información, quienes impartirán las instrucciones de cómo proceder. De haber insertado en la estación de trabajo un disquete o cargado un archivo infectado con algún virus, el programa de antivirus instalado en ella preguntará si interesa escudriñarlo, formatearlo o removerlo. El usuario deberá seleccionar siempre removerlo y avisar de inmediato al Área de Sistemas de Información. Serán impartidas instrucciones de qué hacer con el disquete o archivo. Luego de completar el proceso que indique, el Área de Sistemas de Información notificará a la persona que le entregó o envió el disquete o archivo si estaba infectado por algún virus.

f. Si el archivo o disquete infectado con algún virus es un documento de trabajo de importancia crítica a la OCIF, el Área de Sistemas de Información intentará escudriñarlo y eliminar el virus. Si luego de escudriñarlo, el Área de Sistemas de Información no puede garantizar que pueda eliminar el virus y en ese caso no permitirá que el archivo o disquete sea cargado en ninguna estación de trabajo de la OCIF.

11. Se prohíbe utilizar las facilidades de la OCIF para propagar maliciosa o voluntariamente algún tipo de virus.

ARTÍCULO 13. Medidas de Protección y Custodia de Datos

A. <u>Protección de datos y documentos</u>

El Área de Sistemas de Información será responsable de tomar todas aquellas medidas requeridas para proveer la seguridad necesaria a los sistemas de información. Estas incluyen

antivirus, control de acceso, protocolo, y privilegio al usuario, entre otras.

Toda computadora mostrará una advertencia para el uso de la computadora indicando que está accediendo los sistemas de información propiedad de la OCIF y está obligado a usar el mismo en cumplimento con este **Reglamento.** La misma establece lo siguiente:

> Este equipo electrónico así como los programas y los archivos instalados son parte del Sistema de Información Computadorizado propiedad de la OCIF y sólo se utilizará para fines estrictamente oficiales. La información desarrollada, transmitida o almacenada en el Sistema también es propiedad de la OCIF y estará accesible para ser examinada y utilizada por el personal autorizado por la Oficina. Los usuarios del Sistema no deberán interceptar información que le ha sido restringida. Se prohíbe el envío de, copia de correspondencia electrónica a otras personas sin el conocimiento del remitente. A éste se le deberá notificar, por lo menos, con copia. Cada usuario deberá establecer su contraseña para tener acceso al Sistema. La misma deberá ser cambiada cada 30 días. Se prohíbe revelar la contraseña. Se prohíbe grabar, en cualquier medio removible o en el disco fijo del equipo, programas no autorizados o sin sus debidas licencias. Entiendo las normas citadas y acepto que cualquier violación a las, mismas pueda ser causa suficiente para el inicio de un proceso disciplinario., NOTA: Si está de acuerdo con estas normas, entre su nombre y su contraseña en la próxima pantalla. De no aceptar estas normas no estará autorizado para utilizar este equipo. Favor de presionar el botón de Shutdown en la próxima pantalla.

Los usuarios no podrán alterar o copiar un archivo de computadora de otro usuario sin tener permiso previo de la persona que originó el documento, salvo el mismo esté en un directorio público. Los programas aplicativos y los datos producto de los procesos de sistemas de información son críticos para la operación de la OCIF. Estos residen en los medios magnéticos de los diversos computadores instalados en el Cuarto de Servidores.

El acceso físico al Cuarto de Servidores está restringido a personal autorizado para poder prevenir la destrucción maliciosa o accidental de información, equipos, datos o facilidades, o acciones que puedan, de alguna manera, impedir el funcionamiento correcto y/o manejo de dicho equipos, datos o instalaciones. El acceso al mismo se determinará de tiempo en tiempo mediante los procedimientos que establezca el Comisionado.

B. <u>Resguardo de datos</u>

Los programas y datos pueden perderse por incidentes de cualquier naturaleza, sea natural, accidental o mecánica. La única manera de proveer para su recuperación y restauración

consiste en un proceso de respaldo (backup). Este proceso consiste en copiar los programas aplicativos y los archivos de datos a un medio que permita guardarlos en un sitio protegido. El proceso de respaldo en el caso de la OCIF es copiando en citas magnéticas los programas aplicativos y los archivos de datos en un itinerario establecido y guardándolos en un sitio externo contratado al efecto.

La norma de respaldo de librerías de programas y archivos de datos de la OCIF es hacer copias en cinta cada día hábil y retenerlas durante un periodo establecido en un local protegido y de entrada controlada fuera del edificio en el que está localizado el equipo informático en el que residen los programas y archivos de datos de producción. Para propósitos de control, el recogido, control y custodia de las cintas de respaldo se asignará a personal ajeno a la administración diaria de los servidores. Estas personas pueden ser del Área de Sistemas de Información siempre que no sea el operador de los servidores. Estas personas son en adelante designadas "Custodio" y "Custodio Alterno".

1. Periodos de Retención:

• Cinta diaria	Diez (10) días calendarios
• Cinta del último día hábil del mes	Seis (6) meses
• Cinta del último día hábil del año fiscal	Cinco (5) años

Los programas y datos de archivos de producción son copiados todos los días hábiles a cintas magnéticas utilizando el programa de resguardo autorizado luego del cierre de operaciones. Para propósitos de control, cada cinta tendrá adherido un marbete conteniendo su número de serie, el cual es el mismo asignado por el manufacturero. Es responsabilidad del Custodio o del Custodio Alterno el colocar este marbete y anotar el número de serie al poner cada cinta en uso.

2. Recogido y entrega de cintas

Cada día hábil, el Custodio o Custodio Alterno se personará al Cuarto de Servidores, retirará las cintas correspondientes al día hábil anterior, las rotulará colocándole un marbete en el que le anota la fecha del día hábil a que corresponden y las registrará en la Bitácora de Cintas de Respaldo Enviadas (ver modelo adjunto). En la Bitácora, el Custodio o Custodio Alterno anota el número de serie de las cintas, la fecha de producción, la fecha de ingreso a custodia, periodo de retención, y firma en el espacio provisto. Luego de retirar del servidor las cintas correspondientes al respaldo del día hábil anterior y completar su registro en la Bitácora, el Custodio o Custodio Alterno colocará cintas de reemplazo en el servidor. Estas cintas de reemplazo estarán disponibles en un espacio designado en el Cuarto de Servidores.

3. Custodia de las cintas de respaldo y su retomo al Cuarto de Servidores

La custodia de las cintas de respaldo se mantiene en una caja de seguridad arrendada en la

Sucursal de la Parada 22 del Banco Popular de Puerto Rico. El Custodio o Custodio Alterno transportará las cintas de respaldo hasta la sucursal y, habiendo satisfecho los requisitos de control del banco, las colocará en la caja de seguridad luego de completar la Bitácora de Cintas de Respaldo en Custodia que permanecerá junto a las cintas. En esta Bitácora anotará el número de serie de las cintas, la fecha de producción, la fecha de ingreso en custodia, el periodo de retención y firmará la misma. Luego de completar el ingreso de las cintas, el Custodio o Custodio Alterno retirará de la caja de seguridad las cintas cuyo periodo de respaldo venció. Para mantener control sobre las cintas retiradas, el Custodio o Custodio Alterno anotará la fecha de retiro en el espacio que corresponde a esas cintas en la Bitácora de Cintas de Respaldo en Custodia. Las cintas retiradas serán regresadas por el Custodio o Custodio Alterno al Cuarto de Servidores y las colocará en el espacio designado para las cintas de remplazo para su uso en una ocasión posterior. Para asegurar el uso uniforme de las cintas de reemplazo, el Custodio o Custodio Alterno las mantendrá en secuencia de su retorno de custodia y cada día usará para reemplazo la de fecha de retorno más antigua.

4. Retención de formularios de Bitácora de Cintas de Respaldo

Luego que todas las cintas registradas en un formulario de Bitácora hayan sido retiradas, tal formulario será retenido por el Custodio o Custodio Alterno por el término de un (1) año contado a partir del día hábil que corresponde a la última cinta registrada en un expediente que titulará Registro de Cintas de Respaldo. Transcurrido el año, el Custodio o Custodio Alterno destruirá el formulario.

5. Ausencia del Custodio

El Custodio es responsable de notificar al Custodio Alterno cuando vaya a estar ausente o esté de vacaciones. No obstante, el Custodio Alterno es responsable de estar pendiente en caso de que el Custodio no esté presente y no pueda notificar. En caso de que ambos, el Custodio y el Custodio Alterno estén fuera de la oficina, el Director del Área de Sistemas de Información puede designar a un recurso alterno para subsanar la deficiencia de personal.

6. Fallas en el proceso de respaldo

En caso de que por alguna razón, el proceso de respaldo no sea realizado según dispuesto en estas instrucciones deben tomarse las siguientes medidas:

i. El Custodio o Custodio Alterno informará al personal ubicado en el Cuarto de Servidores la falla técnica del equipo y anotará en la Bitácora si no se produjeron las cintas correspondientes.

ii. De no ser posible guardar las cintas en bóveda en un día determinado, las mismas se guardarán en un archivo cerrado con llaves fuera del área de los servidores. Tales cintas deberán llevarse a la bóveda del banco el próximo día

hábil.

iii. El Custodio o Custodio Alterno informará al Director del Área de Sistemas de Información o al Comité de Tecnología o un representante autorizado sobre cualquier otra causa que impida cumplir con el proceso de respaldo y, si este no está disponible, lo informará al Comisionado.

La seguridad de las aplicaciones pre-programadas la efectuará el funcionario a cargo de la administración, control y custodia de las licencias de las referidas aplicaciones del Área de Sistemas de Información o un representante autorizado.

Cada usuario debe efectuar una producción semanal de copias de reserva (back-ups) de los archivos de información de su computadora en el directorio asignado a cada usuario.

Los usuarios de los sistemas de información deben guardar los documentos en el área designada "public" en los servidores de la OCIF con el fin de protegerlos mediante los mecanismos de resguardo existentes. De esta manera, sus documentos formarán parte del resguardo diario que se realiza a los servidores. Los documentos o datos que sean guardados fuera del área designada, (entiéndase memorias removibles, disco duro de la computadora, discos compactos, etc.), serán responsabilidad del usuario y no serán resguardados por el sistema. Bajo ningún concepto se tratará de recuperar datos y/o documentos que hayan sido guardados fuera del área designada.

Todo usuario de laptop que no esté conectada a la red será responsable de efectuar un proceso de resguardo (backup) en un medio físico externo como CD, DVD o "pen drive". Los discos CD, DVD y "CD-ROM", serán rotulados, protegidos y almacenados en un lugar seguro, manteniendo el sistema de resguardo (back-up) establecido en este **Reglamento**.

Cada usuario es responsable por el buen uso del espacio asignado en los servidores para almacenar sus datos. El mismo es estrictamente para guardar documentos y datos relacionados al trabajo que realiza. Éste no puede utilizarse para almacenar fotos, documentos personales, música y o cualquier otro dato que no esté relacionado a la labor que realiza en la OCIF.

El Director del Área de Sistemas de Información creará y se asegurará del establecimiento y posterior mantenimiento de los archivos de información en casos de desastre. Esta responsabilidad es indelegable por la importancia que reviste para el debido funcionamiento de la estructura organizacional de la OCIF.

C. Archivos de Correo Electrónico

El mantenimiento de los archivos del sistema de correo electrónico es responsabilidad conjunta del Administrador del Sistema y de los usuarios.

1. La OCIF adquirió un sistema de bóveda que almacena copia de todos los correos electrónicos recibido o enviados a través del sistema de correo electrónico de la OCIF. La información recopilada por dicho sistema no puede ser modificada y removida cada cierto tiempo.

2. Los archivos del Sistema de Correo Electrónico serán revisados periódicamente por el Administrador de Correo Electrónico y aquellos usuarios que alcancen el límite máximo de espacio asignado pudieran estar sujetos a la prevención de recepción o envío de mensajes.

3. Los usuarios tendrán un espacio máximo de 1Gb para guardar correos en su Buzón de Correo Electrónico. A aquellos usuarios, que por sus funciones requieren mayor espacio en su buzón, se les asignará hasta un máximo de 5Gb.

4. El usuario es responsable del mantenimiento del tamaño de su archivo de correo electrónico. Cada uno debe procurar la creación de un archivo de resguardo conocido como "PST", para asegurar los mensajes que requieren retenerse por un tiempo indefinido. Además, es responsable por la detección y eliminación de virus que pudieran estar en archivos anexados a mensajes.

4. El límite establecido para el tamaño de los anexos de los mensajes, tanto recibidos como enviados es de 20Mb. Aquellos usuarios cuyas funciones requieran enviar o recibir archivos de mayor tamaño deberán obtener una autorización de su Comisionado Auxiliar, Director o supervisor y coordinar con el área de Sistemas de Información la excepción a esta parte de la política.

5. Los anexos recibidos a través del correo electrónico pudieran contener virus que afecten la operación de sistemas informáticos o que destruyan archivos. La información ejecutable obtenida de fuentes externas no debe ser ejecutada sin previamente cotejar la presencia de virus. Para ayuda en la utilización de programas antivirus, el usuario puede comunicarse con el Área de Sistemas de Información.

6. Los sistemas de correo electrónico serán respaldados diariamente v semanalmente. Los respaldos diarios se retendrán por cinco (5) días, los semanales por el término de cinco (5) semanas y los mensuales por doce (12) meses.

7. Para restablecer los archivos de mensajes electrónicos de los usuarios se requiere justificación sustancial.

8. Toda solicitud para restaurar archivos de correo electrónico, que puede incluir mensajes individuales o archivos de correo completos, tiene que ser sometida al Administrador del Sistema de Correo Electrónico por el Comisionado Auxiliar o Director del área afectada. En la medida que sea posible, las solicitudes deben incluir la siguiente información:

    (1) Nombre del usuario
    (2) Justificación de la petición
    (3) Aprobación del Comisionado Auxiliar o Director del Área
    (4) Requisitos de restablecimiento

9. Bajo ninguna circunstancia se restablecerá un archivo o un mensaje de correo electrónico sin la previa autorización del Administrador del Sistema de Correo Electrónico.

ARTÍCULO 14. Auditoría y Penalidad

La OCIF se reserva el derecho de auditar, vigilar y fiscalizar todos los servicios computadorizados para garantizar que su propiedad sea utilizada solo para propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente, al azar o cuando exista una investigación sobre alguna situación particular. A los empleados no les alberga expectativa de intimidad con relación a cualquier información, documento, mensaje creado, recibido o enviado a través del sistema de información que sea de carácter personal.

Cualquier violación a estas disposiciones estará sujeta a una investigación administrativa, a la suspensión temporera o permanente de servicios de los sistemas de información y/o a la imposición de medidas disciplinarias correspondientes a tenor con el "NORMAS Y PROCEDIMIENTOS SOBRE MEDIDAS CORRECTIVAS Y ACCIONES DISCIPLINARIAS" (Orden Administrativa 2-87 "Normas y Procedimientos sobre Medidas Correctivas) y de la Ley Núm. 4. Además, cualquier persona que viole las reglas establecidas en este Reglamento puede estar sujeta a responsabilidad civil y penal de acuerdo a las leyes estatales y federales aplicables.

Todo usuario cumplirá con los requerimientos de ley referentes al uso, manejo, proceso y custodia de la información contenida en los sistemas electrónicos de información al igual que con cualquier directriz, carta circular, memorial interno o comunicación oficial emitida por la OCIF. De igual forma, el Comisionado exige que todos sus usuarios cumplan cabalmente con las responsabilidades asignadas en las leyes y reglamentos vigentes. Los relevos de responsabilidad no protegen a la OCIF ni al usuario en estos casos.

ARTÍCULO 15. Cláusula de Salvedad

Si cualquier parte, sección, párrafo o cláusula de este **Reglamento** fuera declarado nulo por un

tribunal con competencia, la sentencia no afectará ni invalidará el resto de este **Reglamento**, sino que su efecto quedará limitado a la parte, sección, párrafo o cláusula de este **Reglamento** que hubiese así sido declarado.

ARTÍCULO 16. Vigencia

Este **Reglamento** entrará en vigor inmediatamente.

Aprobado en San Juan, Puerto Rico, hoy 8 de enero de 2014.

LCDO. RAFAEL BLANCO LATORRE
COMISIONADO DE
INSTITUCIONES FINANCIERAS