Departamento de la Familia
Secretaría Auxiliar de Planificación e Informática
Oficina de Sistemas de Información

PLAN DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

NOVIEMBRE 2016

PLAN DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ÍNDICE

		Páginas
I	INTRODUCCIÓN	1
II	BASE LEGAL	1
III	PROPÓSITO	2
IV	APLICABILIDAD	2
V	DEFINICIONES	2
VI	RESPONSABILIDADES	4
VII	MEDIDAS DE SEGURIDAD EXTERNAS	6
VIII	MEDIDAS DE SEGURIDAD INTERNAS	8
	A. Seguridad Física de los Recursos Tecnológicos	8
	B. Seguridad de los Sistemas y Aplicaciones	11
	C. Seguridad de la Redes de Telecomunicaciones	16
	D. Seguridad de la Información	16
	E. Protección del Equipo	17
	F. Resguardo de la Información	18
	G. Protección de los Recursos Humanos	18
IX	RECURSOS ASIGNADOS A LA SEGURIDAD	19
X	ADIESTRAMIENTO	20
XI	CLÁUSULA DE SALVEDAD	21
XII	CLÁUSULA DE SEPARABILIDAD	21
XIII	ENMIENDA	21
XIV	DEROGACIÓN	22
XV	APROBACIÓN Y VIGENCIA	22

APÉNDICES

1. Directrices de Seguridad
2. Registro de Visitantes al Área Común del Data Center de la OSI
3. Registro de Visitantes al Área Administrativa de la OSI
4. Comunicación Control de Acceso al Área de Operaciones de la OSI
5. Registro de Visitantes al Data Center
6. Control de Uso de Llaves Cuartos de Comunicación – OSI
7. Designación de Usuarios Cuentas Administrador de Dominios
8. DEFAM-516, Solicitud de Acceso a los Sistemas
9. DEFAM-517, Solicitud de Acceso al Internet
10. DEFAM-518, Solicitud de Acceso Aplicaciones Especiales-ACUDEN
11. DEFAM-519, Solicitud de Acceso Aplicaciones Especiales-ADFAN
12. DEFAM-520, Solicitud de Acceso Aplicaciones Especiales-ADSEF
13. Empleado Designado a Completar el Formulario DEFAM-82, Certificación Negativa de Acciones de Personal
14. Ejemplo de Alerta Emitido
15. Aviso Inicial en la Pantalla
16. Manual de Normas sobre el Uso de Tecnologías de la Información
17. Manual Operacional sobre Resguardo Recurrente de la Información, Programas de Aplicación y Sistemas Esenciales
18. Registro de Incidencias en Procesos de Resguardo Diario

I. INTRODUCCIÓN

El Departamento de la Familia reconoce la importancia de contar con un Plan de Seguridad de los Sistemas de Información que identifique claramente las medidas establecidas para la protección de la información y los recursos tecnológicos. Constantemente las organizaciones se exponen a sufrir incidentes de seguridad, ya sean internos o externos, causados por personas ya sea voluntaria o involuntariamente, o provocados accidentalmente por catástrofes naturales y fallos técnicos. Es importante concienciar a todo el personal del Departamento sobre la responsabilidad de velar por la seguridad y la integridad de la información y los recursos tecnológicos protegiendo los mismos de daños, destrucción, modificación o divulgación ya sea intencional o accidental.

En virtud de la Ley Núm. 151 del 22 de junio de 2004, conocida como "Ley de Gobierno Electrónico", la Oficina de Sistemas de información (OSI) implementa este Plan de Seguridad cumpliendo con la responsabilidad de orientar y velar porque se cumplan las medidas de seguridad necesarias para salvaguardar los recursos tecnológicos y la información del Departamento de la Familia.

II. BASE LEGAL

A. Plan de Reorganización Núm. 1 del Departamento de la Familia, según enmendado, aprobado el 28 de julio de 1995.

B. Ley Núm. 151 del 22 de junio de 2004, conocida como "Ley de Gobierno Electrónico".

C. Carta Circular Núm. 77-05 de 8 de diciembre de 2004 de la Oficina de Gerencia y Presupuesto (Política TIG-003)

III. PROPÓSITO

Este Plan tiene el propósito de identificar y establecer medidas proactivas para proteger y asegurar la información y los recursos tecnológicos del Departamento de la Familia ante la posibilidad de alguna situación o amenaza que pueda poner en riesgo su integridad y seguridad.

IV. APLICABILIDAD

Este Plan aplica a todos(as) los(as) empleados(as) y funcionarios(as) del Departamento de la Familia, y sus componentes programáticos y operacionales. De igual forma aplica a cualquier consultor(a) o subcontratista que por la naturaleza de sus servicios o de su relación con el Departamento necesite acceder las áreas de tecnología y/o los recursos tecnológicos del mismo. Las medidas de seguridad aquí establecidas servirán de guía al Enlace en Informática en las Administraciones del Departamento, quien debe establecer las medidas adicionales de seguridad física y de protección a los recursos tecnológicos de su Administración que estimen necesarias en su operación.

V. DEFINICIONES

A. Departamento – Se refiere al Departamento de la Familia y sus componentes programáticos y operacionales, tales como: Secretariado, Administración para el Cuidado y Desarrollo Integral de la Niñez (ACUDEN), Administración

de Desarrollo Socioeconómico de la Familia (ADSEF), Administración de Familias y Niños (ADFAN) y la Administración para el Sustento de Menores (ASUME).

B. Secretaria(o) Auxiliar de Planificación e Informática – Persona designada por la Secretaria(o) para planificar, coordinar, dirigir, supervisar y evaluar todas las actividades que se desarrollan en las oficinas adscritas a la Secretaría Auxiliar de Planificación e Informática, entre estas, la Oficina de Sistemas de Información. Participa activamente en la formulación de política pública de su área de trabajo, y en la dirección y supervisión de los proyectos estratégicos de tecnología del Departamento de la Familia.

C. Director(a) de la Oficina de Sistemas de Información – Persona responsable de planificar, organizar, coordinar, dirigir y supervisar todas la operaciones técnicas y administrativas generadas por las unidades de trabajo que integran la Oficina de Sistemas de Información.

D. Enlace en Informática – Titulo funcional de la persona encargada de administrar una red local, ofrecer apoyo tecnológico a los(as) usuarios(as) de una red, administrar contratos de servicios relacionados con la tecnología y coordinar los asuntos relacionados a los sistemas de información de un componente del Departamento (ACUDEN, ADFAN, ASUME y ADSEF).

E. Oficina de Sistemas de Información (OSI) – Oficina adscrita a la Secretaría Auxiliar de Planificación e Informática donde se planifican, organizan, apoyan, dirigen y supervisan las operaciones tecnológicas diarias que apoyan la operación de los componentes del Departamento.

F. Recursos Tecnológicos – Todos los componentes de tecnología que apoyan la operación del Departamento de la Familia, esto incluye, pero sin limitarse, las computadoras, servidores, impresoras, telefonía VoIP, equipo multifuncional, *switches, routers*, cableados, equipo y conexiones inalámbricas, programas, herramientas de oficina, etc.

VI. RESPONSABILIDADES

A. Director(a) de la OSI

1. Preparar y mantener actualizado el Plan de Seguridad de los Sistemas de Información. Este puede delegar la tarea en su representante autorizado(a) y su equipo de trabajo.
2. Divulgar el Plan entre el personal de la OSI.
3. Velar por el buen funcionamiento de los equipos y medidas de seguridad.
4. Adiestrar al personal sobre las medidas de seguridad adoptadas y las responsabilidades que conlleve.

B. Director(a) de la Oficina de Manejo de Emergencias

1. Conocer el contenido del Plan y su participación en caso de ocurrir alguna situación de emergencia que atente contra la seguridad de los recursos tecnológicos relacionada a los sistemas de información.

C. Secretario(a) Auxiliar de Administración y Administradores(as) Auxiliares de Administración

1. Garantizar el mantenimiento de los generadores de electricidad, cisterna de agua, acondicionadores de aire y cualquier otro equipo externo a la

OSI que sea indispensable para el buen funcionamiento de los sistemas de información.

D. Secretarios Auxiliares, Directores(as) y Supervisores(as) de Oficinas

1. Divulgar el Plan entre el personal bajo su supervisión.
2. Velar por el buen uso y la seguridad de los recursos tecnológicos asignados a sus oficinas.

E. Empleados(as) del Departamento de la Familia

1. Velar por el buen uso y la protección de los recursos tecnológicos asignados para su uso. Velar por la seguridad de las aplicaciones, y la información contenida o manejada a través de ellos. Protegerlos contra pérdida, daño o mal uso durante horas regulares de trabajo y dejarlo protegido ante la amenaza de cualquier emergencia prevenible.
2. Aplicar y respetar las medidas de seguridad establecidas por la OSI.

F. Enlace en Informática en las Administraciones

1. Adoptar y atemperar este Plan de Seguridad de los Sistemas de Información a las necesidades de protección de su Administración y establecer las medidas adicionales necesarias para garantizar la seguridad de los recursos tecnológicos y los recursos humanos. Este Plan servirá de guía para las medidas de seguridad a implementar, pero no requiere limitarse a estas.
2. Divulgar el Plan entre su personal y someter evidencia a la OSI.
3. Velar por el buen funcionamiento de los equipos y medidas de seguridad en su Administración.

4. Adiestrar a su personal sobre las medidas de seguridad adoptadas y las responsabilidades que conlleve y mantener evidencia de los mismos.

VII. MEDIDAS DE SEGURIDAD EXTERNAS

La OSI está ubicada en el Edificio Lila Mayoral, Avenida Barbosa 306, Hato Rey, Puerto Rico. Este edificio, donde albergan los recursos de tecnología de información críticos para el Departamento, está físicamente protegido contra las vulnerabilidades que supone una emergencia. El edificio está debidamente preparado con las siguientes medidas de seguridad externas a la OSI que sirven de apoyo ante situaciones de emergencia:

A. Generador o planta eléctrica para emergencias – El edificio cuenta con un generador eléctrico con capacidad de 1,700 kW y un rendimiento operacional de 15 días de servicio por tanque de combustible. Igualmente se cuenta con un tanque de diésel de 5,000 galones. Para este generador existe un contrato de mantenimiento mensual y por lo menos una vez al mes la Oficina de Manejo de Emergencias realiza un simulacro de falla eléctrica.

B. Cisterna – El edificio cuenta con una cisterna con capacidad de almacenamiento de 60,000 galones de agua para satisfacer las necesidades del edificio por diez días de servicio.

C. Prevención de Incendios – El edificio cuenta con un sistema de detectores de humo, alarmas y extintores que alertan sobre la posibilidad de incendio y facilitan el manejo de la situación de manera proactiva. El Departamento tiene contratada a una compañía que monitorea y da mantenimiento a este sistema.

Esta coordinación se hace a través de la Oficina de Manejo de Emergencias del Departamento.

D. Facilidades de estacionamiento – El edificio cuenta con una estructura de nueve niveles con amplia capacidad para estacionamiento, con acceso al mismo a través de dos vías. La primera vía provee acceso al estacionamiento a través de la Ave. Barbosa y hay una segunda vía de acceso a través de la Calle Italia.

E. Guardia de seguridad – El edificio cuenta con servicio de guardia de seguridad tanto para acceso a la periferia como para acceso interno al edificio en turnos de 24 horas al día durante todo el año.

F. Registro de Visitas en Recepción del Edificio – El Departamento cuenta con un componente administrativo adscrito a la Oficina de Seguridad y Manejo de Emergencias que está a cargo de la recepción del edificio. Allí se lleva un registro manual de visitas en donde se identifica a los visitantes con una pegatina especificando el área de servicios a visitar.

G. Registro de Visitas en Recepción de Oficinas – Existen Oficinas que por la naturaleza de sus funciones cuentan con un registro manual de visitas donde los visitantes documentan el propósito de su visita antes de ser atendidos.

H. Acceso controlado a las áreas de trabajo – Existen Oficinas que por la naturaleza de sus funciones cuentan con sistemas de control de acceso mediante tarjetas magnéticas o mediante paneles de contraseñas a las distintas áreas de servicio.

I. Las guías para la protección y vigilancia de los recursos humanos y los activos del Departamento están establecidas en el documento "Directrices de Seguridad"

implementado el 11 de mayo de 2015 en el Departamento de la Familia. En el mismo se establecen las medidas de seguridad a seguir por todos los empleados(as) del Departamento, los(as) guardias de seguridad privados, y los empleados(as) a cargo de la recepción principal. Apéndice 1

Las Administraciones que componen el Departamento de la Familia (ADFAN, ADSEF, ASUME y ACUDEN) deben establecer medidas de seguridad física atemperadas a su realidad operacional con el propósito de proteger sus recursos y activos tecnológicos.

VIII. MEDIDAS DE SEGURIDAD INTERNAS

Además de las medidas de seguridad externas que apoyan la operación de la OSI, existen otras medidas de seguridad internas establecidas para proteger los recursos tecnológicos del Departamento.

A. Seguridad Física de los Recursos Tecnológicos

1. Acceso a la Oficina de Sistemas - El área de Administración y el área de Operaciones en la OSI están protegidas por controles de acceso en las puertas de entrada. En ambas áreas se mantiene un registro manual de visitas donde los visitantes registran su entrada y documentan el propósito de su visita antes de ser atendidos. Apéndice 2 y 3

2. Acceso al cuarto de servidores y equipo de telecomunicaciones - Los servidores y los equipos de telecomunicaciones ubicados en la OSI están separados en un cuarto y protegidos por controles de acceso. La puerta cuenta con un panel numérico con contraseñas autorizadas solo para aquellos(as) empleados(as) cuyas funciones son inherentes a la

operación. El 6 de julio de 2015 se aprobó y tramitó una comunicación del Director de Sistemas de Información impartiendo las directrices sobre el control de acceso al área de operaciones de la Oficina. Apéndice 4

3. El acceso físico al área de servidores está restringida al personal autorizado solamente. En caso de que se tenga que atender alguna situación en esa área por algún recurso externo, la Oficina cuenta con un registro de visitantes al área de servidores y telecomunicaciones donde se registran las entradas y el propósito de las mismas. El recurso es escoltado en todo momento por personal de la OSI. Apéndice 5

4. Acceso a los cuartos de data – En cada piso del edificio hay un cuarto de comunicaciones donde están conectados los "*switches*" de comunicación que permiten interconectar los equipos del Departamento para viabilizar el flujo de la data a través de estos. Estos cuartos están protegidos por una puerta bajo llave a la cual tienen acceso solo el personal de la OSI y de la Oficina de Manejo de Emergencias. La llave se guarda en una caja de seguridad y se mantiene un registro de las personas que solicitan la llave y acceden al área. Apéndice 6

5. Fuentes de Energía Alterna (UPS) - Unidades de suministro de energía de apoyo (UPS) - El cuarto de los servidores cuenta con un sistema de suministro de energía alterna (UPS) que permiten la desactivación de los equipos adecuadamente en caso de que ocurra un fallo en el servicio de energía eléctrica. En promedio estos equipos proveen dos (2) horas

adicionales de corriente que permiten una suspensión ordenada y segura de operaciones, que salvaguarden la integridad de la data procesada y el funcionamiento de los equipos. Esta unidad es la tercera fuente de alimentación de corriente eléctrica y entra en función una vez el generador del edificio deja de funcionar o haya fallado en su arranque, luego de una falla o apagón en el suministro de energía eléctrica.

6. Sistema de Monitoreo de Humedad y Temperaturas - La OSI tiene instalados en el cuarto de servidores herramientas de monitoreo que detectan y alertan sobre problemas de humedad y cambios de temperatura. Este sistema nos ayuda a evaluar el funcionamiento diario de las unidades de aire acondicionado e identificar cualquier anomalía en la temperatura del cuarto de servidores.

7. Unidades de acondicionadores de aire independientes – El cuarto de servidores cuenta con dos sistemas de acondicionador de aire para el control de la temperatura. En caso de falla, el sistema levanta una alarma indicando la anomalía correspondiente. En el interés de garantizar redundancia en el sistema de enfriamiento se instaló una unidad de acondicionador de aire independiente de la unidad central que automáticamente se activa cuando la temperatura del centro de cómputos llega a los 70 grados. Esta unidad entra en función solo si la unidad central del edificio deja de funcionar o falla en su arranque.

8. Extintores de Incendio – La OSI cuenta con extintores de incendio y un sistema de seguridad contra incendios FM200 para equipos electrónicos.

Los extintores están ubicados en áreas visibles, de fácil acceso y sin obstáculos. Estos son revisados anualmente por la Oficina de Servicios Generales para garantizar su vigencia.

9. Ubicación de la Oficina – La OSI está ubicada en el 4to piso del edificio. Esta ubicación provee unas salvaguardas adicionales, ya que minimiza la vulnerabilidad y la exposición de los recursos a daños por inundaciones, filtraciones por ventanas, exposición a visitantes o personas ajenas a la Oficina, entre otras.

B. **Seguridad de los Sistemas y Aplicaciones**

1. Acceso a los Servidores

Los servidores están protegidos por una cuenta de administrador a la que solo tiene acceso el personal designado en la Oficina de Sistemas conforme definido en los privilegios de acceso del grupo "Domain Admin". La clave de acceso (*password*) de la cuenta de administrador de sistema está en un sobre lacrado guardado en una bóveda a prueba de fuego en la Oficina de Finanzas. El grupo "Domain Admin" cuenta con atributos de administrador y el permiso se prepara por escrito con la autorización del (la) Director(a) de la OSI para la sana administración de la seguridad en la red. Apéndice 7

2. Monitoreo diario de los Servidores

Diariamente el administrador de la red coteja mediante una herramienta de monitoreo, los registros de eventos para tomar las medidas correctivas que se requieran. La verificación o cotejo diario de los

servidores ayuda a prevenir o minimizar el impacto de problemas en la red. Los eventos se catalogan en tres categorías:

Las categorías de los mensajes aquí registrados son:

Error: Identifica los problemas que están ocurriendo y que requieren atención inmediata

Warning: Identifica situaciones que pueden convertirse en problemas futuros. (Advertencias)

Information: Notifica que alguna operación se completó satisfactoriamente. No es tan crucial como los anteriores.

3. Monitoreo de Virus, *Malware* e Intrusos - (*Firewalls*)

La OSI en su objetivo de brindar protección a los activos informáticos, cuenta con equipos y herramientas "software" capaces de monitorear y detectar amenazas que ponen en riesgo la seguridad de los sistemas de información del Departamento. Para lograr los objetivos antes descritos, contamos con la herramienta de *Microsoft System Center* 2012 R2, configurada para prevenir, detectar y eliminar virus informáticos o *malware* de forma inmediata en computadoras o servidores dentro de la red de computadoras del Departamento. Con el mismo objetivo, contamos con herramientas a*nti-spam* que impiden la entrada de correos electrónicos no deseados además de proveer protección contra "phishing" o sitios *web* que solicitan información personal. Con el fin de brindar protección perimetral en las comunicaciones tanto internas como externas, contamos con equipos "firewalls" con la capacidad de gestionar y filtrar la totalidad del tráfico de comunicación bidireccionalmente. Mediante el mecanismo de reglas, se define específicamente quién entra o quien sale a la red. El

equipo utilizado para estos fines es un *firewall FortiGate* con licencia de filtrado *web*.

4. Uso de Contraseñas de acceso a los sistemas

   1. Acceso a la red de telecomunicaciones – Todo(a) empleado(a) que tiene acceso a los equipos y programas del Departamento tiene que tener una cuenta creada en la OSI. Para la creación de esta cuenta se requiere completar el formulario "Solicitud de Acceso a los Sistemas", DEFAM-516. La misma debe estar aprobada por el Director(a) o Supervisor(a) directo del empleado(a). Apéndice 8
   2. Privilegios de acceso a las aplicaciones y herramienta - Es responsabilidad del (la) Director(a) de la oficina solicitante o supervisor(a) del(de la) empleado(a), solicitar los privilegios de uso de las aplicaciones y herramientas disponibles a través de la red. Para la autorización de los distintos accesos se utilizan los siguientes formularios. DEFAM-517, Solicitud de Acceso a Internet; DEFAM-518, Solicitud de Acceso Aplicaciones Especiales-ACUDEN; DEFAM-519, Solicitud de Acceso Aplicaciones Especiales-ADFAN; DEFAM-520, Solicitud de Acceso Aplicaciones Especiales-ADSEF. Apéndice 9, 10, 11 y 12. A cada usuario(a) de los sistemas de información se les crea una cuenta que consiste de una combinación de nombre de usuario y una contraseña para acceder los sistemas. Las contraseñas de usuario se utilizarán solamente para el uso del (la) empleado(a) al

que se le emitió. El usuario(a) es responsable de proteger su cuenta/contraseña y de cada actividad registrada en el sistema bajo su cuenta.

3. Cambio de contraseñas - Con el propósito de mantener la seguridad en las cuentas de usuarios se establece una política automática a nivel de sistemas que obliga a él (la) empleado(a) a cambiar su contraseña de acceso un mínimo de cada 180 días y bajo unos parámetros previamente definidos.

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	5 passwords remembered
Maximum password age	180 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

5. Desactivación de cuentas

El proceso de desactivar una cuenta de usuario entra en efecto cuando el(la) empleado(a) renuncia, termina contrato, se traslada o cualquier otra acción que lo separe de su área de trabajo permanentemente. Para esto, el(la) empleado(a) completa el formulario DEFAM-82, Certificación Negativa de Acciones de Personal. Esta es requerida por la Oficina de Recursos Humanos y tiene el propósito de que las áreas de trabajo determinadas den su visto bueno, con el cual certifican que el(la) empleado(a) entregó todos los recursos asignados para su uso durante la vigencia de su nombramiento o toman nota para posteriormente llevar a cabo alguna acción. Una de las partes en este documento requiere

presentar el formulario ante la OSI para que el(a) empleado(a) autorizado(a) verifique las cuentas de acceso asignadas al usuario en los sistemas, inactive las mismas y certifique en el documento que el(la) empleado(a) fue liberado(a) de sus responsabilidades con la OSI. Apéndice 13.

6. Manejo de Licencias de Programas y Herramientas de Oficina

Todos los(as) usuarios(as) son responsables de usar sus sistemas de información con la configuración instalada por la OSI. Esta Oficina es la única autorizada a instalar programas, herramientas de oficina y actualizaciones de licencias en las computadoras y servidores del Departamento. Los mismos tienen que haber sido legalmente adquiridos mediante los procesos de compra del Departamento, o a través de los programas de licenciamiento de productos disponibles a través de la Oficina de Gerencia y Presupuesto del Estado Libre Asociado de Puerto Rico. La piratería de *software* está completamente prohibida en el Departamento. Ningún empleado(a) del Departamento está autorizado(a) ni debe tener privilegios de administrador(a) local de su computadora que le permitan instalar herramientas personales y/o bajar herramientas gratuitas de internet sin la previa evaluación y autorización de la OSI. Esto con el propósito de proteger de virus los recursos del Departamento y mantener la seguridad de los mismos.

C. **Seguridad de las redes de telecomunicaciones**

1. Red Primaria de Telecomunicaciones - La red primaria de telecomunicaciones del Departamento cuenta con un servicio externo de monitoreo remoto los 7 días de la semana. La herramienta de monitoreo utilizada es *Solarwinds*. Este servicio es contratado como parte del servicio a la red primaria de telecomunicaciones para asegurar la disponibilidad y el funcionamiento continuo de la misma. La compañía contratada genera alertas para el Departamento mediante el envío de correos electrónicos en caso de que se interrumpa alguna conexión en cualquier localidad del Departamento a nivel isla. Igualmente se hace reporte cuando las mismas entran en función nuevamente. Apéndice 14

D. **Seguridad de la Información**

1. Propiedad de la Información – Todo(a) empleado(a) que pretende acceder una computadora en el Departamento es apercibido mediante un aviso inicial en la pantalla, de que toda la información manejada y almacenada en los recursos tecnológicos del Departamento, así como todos los mensajes transmitidos a través de estos, son propiedad del Departamento. Apéndice 15

   Este mensaje tiene que ser aceptado por el usuario(a) antes de poder acceder con su contraseña asignada. De lo contrario no se permite la entrada a los sistemas.

2. Protección de la información - Todo el personal es responsable de asegurar que no ocurra divulgación accidental, modificación o pérdida de información confidencial. Información confidencial incluye información de los beneficiarios, información oficial y relaciones confidenciales del Departamento o su personal. Los usuarios(as) deben proteger su acceso desactivándose cada vez que dejan su estación de trabajo, de manera que se pueda prevenir la divulgación no autorizada o acceso a la información por personas no autorizadas. Cualquier computadora que se deje sin atender por más de diez (10) minutos, será automáticamente desactivada. El usuario(a) será responsable de cualquier evento que ocurra si deja su estación activa y desatendida.

E. **Protección del Equipo**

1. Todo el personal que utilice cualquier tipo de equipo de sistemas de información como parte de sus funciones diarias, es responsable por dicho equipo y de protegerlo contra pérdida, daño o mal uso durante horas regulares de trabajo. Igualmente es responsable de mantenerlo en un lugar seguro fuera de horas de trabajo si es equipo portátil. Existe en cada oficina un encargado interno de la propiedad quien es responsable de velar por el movimiento y la seguridad del equipo tecnológico asignado a la oficina.

2. **Manual Sobre el Uso de las Tecnologías de la Información** – En junio 2015 se aprobó y distribuyó el "Manual de Normas sobre el Uso de

Tecnologías de Información". El mismo establece las normas sobre administración, uso y conservación de los recursos tecnológicos del Departamento. Apéndice 16

F. **Resguardo de la información** – Efectuar resguardo de la información en los servidores en forma diaria previene el riesgo de perder la misma como consecuencia del equipo, virus, fallas de corriente, problemas en la red, entre otros. La operación del resguardo (*backup*) se ejecuta diariamente y se mantiene en un equipo de almacenamiento externo ubicado en la OSI. En mayo 2016 se aprobó el "Manual Operacional sobre Resguardo Recurrente de la Información, Programas de Aplicación y Sistemas Esenciales", el cual contiene normas específicas relacionadas a este proceso. Apéndice 17 El área de operaciones de la OSI mantiene un registro diario de eventos con el propósito de documentar aquellas instancias en las que los procesos de resguardo se ven afectados por algún evento. Igualmente se documenta en el registro la acción tomada para corregir la situación. Apéndice 18

G. **Protección de los Recursos Humanos**

En este Plan se detallan medidas respecto al registro de visitantes, controles de acceso físico a las áreas de sistemas y servicios de guardia de seguridad que garantizan la protección de los(as) empleados(as). Además de estas medidas, el Departamento, a través de la Oficina de Manejo de Emergencias, ha establecido un Plan de Desalojo del edificio en caso de alguna amenaza o emergencia. El mismo tiene aplicabilidad

a todos(a) los(as) empleados(as) del Departamento. La OSI se ciñe a este Plan conforme establecido.

IX. RECURSOS ASIGNADOS A LA SEGURIDAD

1. **Personal de Respuesta de la OSI** - La OSI cuenta con personal identificado para hacer la función de personal de respuesta inmediata antes, durante y después de algún evento que pueda poner en riesgo la seguridad de los recursos tecnológicos del Departamento. Este personal evaluador consta del Director(a) de la OSI, así como dos (2) supervisores(as) en puestos gerenciales. Igualmente son responsables de apoyar a este grupo los Enlaces en Tecnología de las Administraciones del Departamento.

2. **Personal contacto manejo de emergencias**. Además del personal de respuesta descrito anteriormente, se ha identificado en cada uno de los componentes operacionales de la OSI, personal que se activa, se involucra y apoya en la recuperación de la normalidad de las operaciones de la Oficina, si estas se afectaran de alguna manera. Estos son el(la) Supervisor(a) de Equipo de Procesar Datos, el(la) Supervisor(a) de Sistemas II y el(la) Técnico(a) de Redes y Telecomunicaciones.

3. **Encargado Interno de la Propiedad.** La OSI cuenta con un(a) encargado(a) interno de la propiedad que maneja los movimientos, la verificación y la transferencia de equipos electrónicos. Esto provee unas garantías adicionales de manejo y control de los recursos de tecnología.

4. **Participación de la Oficina de Manejo de Emergencias**. En caso de algún evento catalogado como emergencia por la Oficina de Manejo de Emergencias del Departamento, en el cual se prevea algún daño potencial a los recursos tecnológicos del Departamento, la OSI queda activada conforme establecido en el Plan de Emergencias de Desastres del Departamento.

X. ADIESTRAMIENTO

A. Una vez aprobado el Plan de Seguridad de los Sistemas de Información, por el/la Secretaria del Departamento, el(la) Director(a) de la OSI deberá ofrecer un adiestramiento para el personal bajo su supervisión y contratistas ubicados(as) en dicha Oficina. Esta acción puede ser delegada a un(a) representante autorizado(a) de la propia Oficina. El adiestramiento debe ofrecerse no más tarde de 60 días laborables luego de aprobado y divulgado el Plan. Así mismo, cada vez que el Plan sea actualizado, debe informarse y distribuirse al personal de la OSI y conforme la magnitud de los cambios determinar si es necesario el readiestramiento.

B. El Plan de adiestramientos estará segmentado y diseñado de acuerdo a las tareas y responsabilidades de cada funcionario(a) a cargo de la seguridad y la protección de los recursos tecnológicos. Ejemplo:

1. El personal a cargo de la seguridad de las aplicaciones será adiestrado sobre los procesos de altas y bajas de usuarios para uso a las aplicaciones y los niveles de acceso de acuerdo a sus funciones, la importancia de mantener la documentación, entre otros.

2. El personal que administra los servidores será adiestrado sobre los procesos para la creación de usuarios en el sistema, la aplicación sistemas de antivirus, procesos de actualización de ambientes operacionales, etc.
3. Los usuarios(as) de los recursos tecnológicos serán adiestrados en temas de protección de la información, protección del equipo, uso y protección de sus contraseñas, etc.

C. A los(as) empleados(as) de nuevo nombramiento y/o a los consultores(as) contratados en la OSI se le entregará copia del Plan y se requerirá acuse de recibo que se mantendrá como evidencia. Igualmente, se les orientará sobre la disponibilidad para clarificarles cualquier duda que les pueda surgir.

XI. CLÁUSULA DE SALVEDAD

La Autoridad Nominadora es la responsable de resolver cualquier situación que no esté contemplada en este documento.

XII. CLÁUSULA DE SEPARABILIDAD

La nulidad de alguna de las partes o disposiciones de este Plan no afectará las otras que puedan ser válidas, independientemente de las declaradas nulas.

XIII. ENMIENDA

La enmienda o actualización de este Plan está delegada al(a la) Director(a) de la OSI, adscrita a la Secretaría Auxiliar de Planificación e Informática. El Plan puede ser enmendado por recomendación del Director(a) de la OSI, o por disposición del

Secretario(a) o representante autorizado(a) del Departamento, cuando se determine necesario.

XIV. DEROGACIÓN

Este Plan deroga el "Plan de Seguridad de los Sistemas de Información de la Agencia 2011", de OSI-Secretariado, aprobado el 28 de enero de 2011, por la entonces Secretaria Auxiliar de Planificación e Informática, y el Director Interino de la Oficina de Sistemas de Información. Igualmente deroga el "Manual de Seguridad de acceso a la Red" aprobado el 24 de febrero de 2011, por el entonces Director de OSI-Minillas. Ambas Oficinas fueron fusionadas en el año 2013 y sus operaciones fueron consolidadas como un solo componente ubicado en el Secretariado del Departamento de la Familia.

XV. APROBACIÓN Y VIGENCIA

Este Manual entra en vigor a partir de la fecha de aprobación y firma por el(la) Secretaria(o) del Departamento de la Familia y mantendrá vigencia hasta el momento que se someta y se apruebe alguna enmienda al mismo.

Idalia Colón Rondón, MTS
Secretaria

7 noviembre 2016
Fecha

APÉNDICE 1

DIRECTRICES DE SEGURIDAD

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

11 de mayo de 2015

A TODO EL PERSONAL DEL SECRETARIADO Y DE LA ADFAN

DIRECTRICES DE SEGURIDAD A SEGUIR EN EL DEPARTAMENTO DE LA FAMILIA EDIFICIO LILA MAYORAL

A partir del lunes, 11 de mayo de 2015, se implementaron las nuevas Directrices de Seguridad en el Edificio Lila Mayoral del Departamento de la Familia.

Las nuevas normas a seguir por todos los(as) empleados(as) del departamento con acceso al edificio establecen lo siguiente:

a. Todo empleado que labore en el edificio deberá tener accesible su identificación con foto para propósitos de facilitar la identificación del personal autorizado en la recepción. Empleados sin tarjeta de identificación deberán registrarse en el libro de visitas diarias.

b. Todo(a) empleado(a) que abandone el edificio posterior a su horario regular de salida debe firmar el registro de salidas de empleados a partir de las 5:00 pm. Esta norma es para todos los(as) empleados(as).

c. Todo(a) supervisor(a) o director(a) de oficina que requiera que un(a) empleado(a) permanezca en el edificio fuera de horas laborables deberá solicitar la autorización para el debido proceso de acceso. Dicha autorización es concedida por la directora de la Oficina de Seguridad quien, para garantizar la seguridad del personal, notificará al personal de vigilancia interna la permanencia de empleados en el edificio.

d. Todo(a) supervisor(a) o director(a) de oficina que requiera que un(a) empleado(a) labore durante fines de semanas y/o días feriados deberá solicitar la autorización para el debido proceso de acceso. Deberá solicitar, mediante comunicación escrita o correo electrónico a la Oficina de Seguridad y Manejo de Emergencias.

De igual manera, se señala algunas directrices que debe conocer para beneficio y brindar ayuda a visitantes.

a. El personal de recepción solicitará una identificación con foto válida a toda persona que solicite autorización para entrar al edificio en busca de recibir, dar servicios, acudir a cita y/o reunión, entregar documentos o cualquier otro asunto.

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

b. Cada piso de nuestro edificio será identificado por colores para propósito de identificar visitantes en los pisos correspondientes. El personal de recepción proveerá una pegatina a cada visitante. Esta pegatina será del color del piso a visitar en los que se incluye a personas en salones de adiestramientos. Esta pegatina ayudará al personal de seguridad a identificar visitantes no autorizados a otras áreas, por lo que como empleados(as) recomendamos brindar ayuda a estos visitantes o notificar a la Oficina de Seguridad si sospecha de alguna situación referente a visitantes fuera de área.

Agradeceré el fiel cumplimiento de las nuevas directrices.

Idalia Colón Rondón, MTS
Secretaria

DIRECTRICES DE SEGURIDAD

DEPARTAMENTO DE LA FAMILIA
EDIFICIO LILA MAYORAL

Con el propósito de garantizar la seguridad de los empleados(as), visitantes, propiedad, planta física y estacionamiento del edificio, se imparten las siguientes directrices:

1. Guardias de Seguridad Privada

El edificio del Departamento de la Familia posee dos entradas que son utilizadas para el acceso peatonal y vehicular. La entrada principal tiene acceso por la Avenida Barbosa. La misma permite la entrada vehicular; no obstante, no se permite la salida de vehículos por la misma. La segunda entrada, por el lado posterior, tiene acceso a la calle Italia. Ambas entradas son custodiadas por guardias de la seguridad privada.

a. Todo visitante será recibido de forma cortés y atendido con respeto.

b. El guardia de la seguridad privada que se ubica en la caseta Italia estará a cargo del registro vehicular de todo visitante que utilice esa entrada y del registro de empleados autorizados a utilizar vehículos del Departamento para salidas oficiales.

c. El guardia de la seguridad privada que se ubica en la caseta Barbosa estará a cargo del registro vehicular de todo visitante que utilice esa entrada.

d. El personal asignado a ambas casetas utilizará los formularios "*Registro Vehicular de Visitantes*" y "*Registro de Automóviles y Conductores Autorizados a Conducirlos*". (Se anejan documentos en referencia)

   1) Registro Vehicular de Visitantes

   2) Registro de Automóviles y Conductores Autorizados a Conducirlos

e. De igual modo, se registran los guardias de la seguridad privada en turnos en la hoja provista por la Compañía contratada identificada como Asistencia Diaria y codificada ADM-F-20-A9 A(Se aneja el documento en referencia)

f. El guardia de la seguridad privada asignado a la ronda y otras áreas del

edificio, incluyendo la seguridad de la Unidad de Investigaciones Especiales (UIE), estará en vigilancia continua y deberá notificar a través de sus radios transmisores cualquier situación e incidente que requiera la debida intervención del personal de la Oficina de Seguridad y Manejo de Emergencias, de la Oficina del Secretario Auxiliar de Administración, de la Oficina de la Secretaria o de la Oficina de la Subsecretaria.

g. El personal de la seguridad privada que atienda cualquier hecho suscitado dentro de las facilidades del edificio, estacionamiento, área de la UIE, alrededores del edificio; incluyendo situaciones de protesta, accidentes, hurtos o cualquier otra circunstancia presentada por empleados(as) y visitantes preparará un informe escrito el mismo día del incidente, para lo cual utilizará el formulario "*Informe de Incidencias*", documento interno que utiliza la compañía de seguridad Privada (Se aneja documento en referencia).

   Una vez realizado el informe deberá tramitarlo a su supervisor(a) inmediato(a), quien radicará cualquier otro informe, de ser necesario, y entregará los documentos el mismo día del incidente a la Oficina de Seguridad y Manejo de Emergencias.

h. En caso de robo, vandalismo, escalamiento, accidentes, caídas o algún tipo de accidente o situación de riesgo, peligro, daño o pérdidas en las que resulte perjudicado un(a) visitante, un(a) empleada o algún área de trabajo dentro de las facilidades o sus alrededores, incluyendo el estacionamiento; el personal de la Oficina de Seguridad y Vigilancia del Secretariado debe personarse al lugar de los hechos y una vez controlada la situación debe completar el formulario "*Informe de Incidentes*", DEFAM-440(Se aneja documento en referencia. Este informe se realiza en presencia de las partes involucradas; y en casos, cuando es el resultado de pérdidas, en presencia del personal de seguridad privada y de testigos, de haber alguno.

i. El DEFAM-440, *Informe de Incidentes*, también deberá ser utilizado en situaciones de protesta y manifestaciones presentadas en los alrededores, siempre y cuando el personal de seguridad, entiéndase guardias y personal de la Oficina de Seguridad y Vigilancia del Departamento, intervengan con el o los manifestantes.

j. En el informe se detallará el hecho suscitado, la intervención, el manejo del asunto, los resultados y/o cualquier directriz o acción tomada ante la eventualidad.

k. Cualquier situación presentada fuera de horas laborables será manejada por el personal de seguridad privada, incluido el guardia asignado a la UIE. El guardia de la seguridad privada informará al personal de la Oficina de Seguridad y Manejo de Emergencia sobre la situación y manejará la situación hasta que el personal de la Oficina de Seguridad y Manejo de Emergencia o quien se determine intervendrá con la situación se presente al edificio.

2. Recepción

a. La(El) recepcionista o cualquier otro personal que la sustituya, atenderá la recepción principal del Departamento de forma cortés y con el respeto que merece todo(a) empleado(a) y visitante que acuda a nuestra dependencia diariamente.

b. La(El) recepcionista solicitará una identificación con foto válida a toda persona que solicite autorización para entrar al edificio en busca de recibir o dar servicios, acudir a cita o reunión, entregar documentos o cualquier otro asunto.

c. La(El) recepcionista deberá anotar la información de todo visitante en el formulario *"Registro de Visitas Diarias"(Se aneja documento en referencia)*, con excepción de aquellos que visitarán los salones de adiestramiento.

d. La(El) recepcionista le proveerá una pegatina a cada visitante, la cual será impresa en siete colores diferentes. Cada piso estará identificado con un color y los salones de adiestramiento. Esta pegatina ayudará al personal de seguridad y empleados(as) a identificar visitantes no autorizados a otras áreas.

e. Toda persona que requiera visitar la Oficina de la Secretaria, Subsecretaria, División Legal, Secretaria Auxiliar de Planificación, Oficina de Prensa al

igual que la Oficina de la Administradora de la ADFAN, deberá ser anunciada a la oficina indicada para autorización de acceso al área solicitada.

f. Cualquier situación referente a visitantes sospechosos deberá ser notificada al personal de seguridad privada y a la Oficina de Seguridad y Manejo de Emergencias. La notificación deberá ser realizada a través de los radios comunicadores o a través del cuadro telefónico, según lo amerite la circunstancia.

g. Cuando la(el) recepcionista entienda que requiere de la presencia del personal de seguridad privada o la escolta de cualquier visitante a oficinas, deberá solicitarlo inmediatamente y notificar a la Oficina de Seguridad y Manejo de Emergencias sobre la situación.

h. Todo empleado que labore en el edificio deberá tener accesible su identificación para propósitos de facilitar la identificación del personal autorizado a entrar al edificio sin la debida registración requerida.

i. Toda persona visitante que acuda a nuestro edificio para tomar talleres o adiestramientos programados deberá ser orientado por la(el) recepcionista o por un ujjier de haber sido establecido el mismo sobre la ubicación del lugar a visitar.

j. El personal encargado del taller y/o adiestramiento será responsable de entregar copia de la "Hoja de Asistencia" en la recepción una vez finalizado el taller para propósitos del registro diario de visitantes del edificio.

k. Todo(a) empleado(a) que abandone el edificio posterior a su horario regular de salida debe firmar el registro de salidas de empleados 5:00pm en adelante (Se aneja documento en referencia) ubicado en la recepción. (Esto no aplica a personal de confianza)

l. Todo(a) supervisor(a) o director(a) que requiera que un empleado(a) permanezca en el edificio fuera de horas laborables deberá notificar a la Oficina de Seguridad y Manejo de Emergencias para el debido proceso de

acceso y autorización. La solicitud debe realizarse por comunicación escrita o mediante correo electrónico dirigido al(a la) Director(a) de Seguridad y Manejo de Emergencias. Esto incluye acceso para fines de semanas y días feriados.

a. El personal a cargo de coordinar servicios o trabajos deberá solicitar, mediante comunicación escrita o correo electrónico a la Oficina de Seguridad y Manejo de Emergencias, autorización para el acceso de personas de compañías privadas que realizarán labores de reparación, limpieza, entre otras, durante fines de semanas, días feriados o fuera de horas laborales en semana. Además, debe informar sobre aquellas labores que puedan propiciar incidentes relacionados con la activación de la alarma de aviso de incendios u otros asuntos relacionados, como olores objetables y otros que puedan poner en riesgo la salud y seguridad del personal o visitantes.

Idalia Colón Rondón, MTS
Secretaria

Carmen M. Agosto Serrano, MBA, BSW
Directora
Oficina de Seguridad y Manejo de Emergencias

Aprobado: 11 de mayo de 2015

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

ESTADO LIBRE ASOCIADO DE PUERTO RICO
DEPARTAMENTO DE LA FAMILIA
UNIDAD DE TRANSPORTACION
REGISTRO DE AUTOMOVILES Y CONDUCTORES
AUTORIZADOS A CONDUCIRLOS

FECHA: _____

NOMBRE DEL CONDUCTOR	OFICINA	RUTA	TABLILLA	CANTIDA DE GASOLINA 1.SALIDA 2. ENTRADA	1.HORA 2.MILLAJE DE SALIDA	1.HORA 2.MILLAJE DE ENTRADA	FIRMA DEL CONDUCTOR
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	

REGISTRO DE GUARDIANES Y TURNOS CORRESPONDIENTES

FIRMA DEL GUARDIAN PRIMER TURNO	HORARIO	FIRMA DEL GUARDIAN SEGUNDO TURNO	HORAIO	FIRMA DEL GUARDIAN TERCER TURNO	HORARIO	COMENTARIO

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

REGISTRO VEHICULAR DE VISITANTES

Departamento de la Familia
Oficina de Manejo de Emergencias y Seguridad

Fecha	Nombre en letra de molde	HORA	Oficina a Visitar	Propósito de la Visita	Número de Tablilla	Marca Vehículo	PISO

NOMBRE: _____
FIRMA: _____
PUESTO: _____
FECHA: _____

ASISTENCIA DIARIA

A= ARMADO
D= DESARMADO

FECHA	TOTAL HORAS	NOMBRE EMPLEADO	A/D	TURNO ENTRADA	TURNO SALIDA	#EMP	FIRMA EMPLEADO	SUP
LUN___								
T.Hrs___								
MAR___								
T.Hrs___								
MIE___								
T.Hrs___								
JUE___								
T.Hrs___								
VIE___								
T.Hrs___								
SAB___								
T.Hrs___								
DOM___								
T.Hrs___								

HRS A: _____ HRS D: _____ TOTAL HRS: _____

_____
FIRMA DEL SUPERVISOR

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

Genesis Security Services, Inc.
5900 Ave. Isla Verde L-2 PMB 438 Carolina, P.R. 00979
TEL. (787) 776-2381 / FAX (787) 757-8975

INFORME DE INCIDENCIA # 20728

1. Nombre del Guardián: _____ Núm. Emp. _____
2. Nombre del Supervisor: _____
3. Fecha del Incidente: _____ Hora del Incidente: _____
4. Lugar del Puesto: _____
5. Narrativa del Incidente:

_____

6. Descripción de las lesiones corporales y/o daños a la propiedad, si alguno:

_____

7. Nombre de (los) testigo (s): Dirección y Teléfono:

_____

8. Nombre del Agente: _____ Núm. Placa: _____
9. Número de Querella: _____ Precinto: _____
10. Informe entregado a: _____

_____ Firma del Guardián

_____ Fecha

DEFAM-440
SP-02/08

Estado Libre Asociado de Puerto Rico
DEPARTAMENTO DE LA FAMILIA
División de Seguridad y Vigilancia

☐ Secretariado
☐ Administración: _____

INFORME DE INCIDENTES
(Ver instrucciones al dorso)

1. Nombre de la persona o área perjudicada:

2. Grupo al que pertenece: ☐ Empleado(a) ☐ Visitante ☐ Área de trabajo

3. Si es **empleado(a)**, provea la siguiente información:
Puesto que ocupa: _____
Oficina donde trabaja: _____ Teléfono: _____
Si es **visitante**, provea la siguiente información:
Dirección Postal: _____
Teléfono: _____ Otro: _____

4. Fecha del incidente:	5. Hora del incidente:	6. Lugar del incidente:

7. Tipo de incidente:
☐ Vandalismo ☐ Escalamiento ☐ Robo ☐ Fuego ☐ Caída
☐ Otro: _____

8. Persona(s) Testigo(s):		☐ Empleado(a) ☐ Visitante
		☐ Empleado(a) ☐ Visitante

9. Describa brevemente el incidente. De necesitar más espacio, puede utilizar una hoja de papel y graparla a este formulario.

10. Algún otro comentario respecto al incidente:

11. _____ _____
Nombre y firma de persona perjudicada — Fecha

12. _____ _____
Nombre y firma del(de la) Guardia de Seguridad — Fecha

13. _____ _____
Nombre y firma del(de la) Supervisor(a) de Seguridad y Vigilancia — Fecha

Período de Retención: Dos (2) años, previa autorización del(de la) Supervisor(a) de Seguridad y Vigilancia.

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

REGISTRO DE VISITAS DIARIAS

Departamento de la Familia
Oficina de Seguridad y Manejo de Emergencias

FECHA	Hora Entrada	Hora Salida	NOMBRE DEL VISITANTE	OFICINA A VISITAR Y NUM. DE PISO	NUM. DE IDENTIFICACION	PROPOSITO DE LA VISITA

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

PISO 1

FAMILIA

Nombre Visitante

Fecha

PISO 2

FAMILIA

Nombre Visitante

Fecha

PISO 3

FAMILIA

Nombre Visitante

Fecha

PISO 4

FAMILIA

Nombre Visitante

Fecha

PISO 5

FAMILIA

Nombre Visitante

Fecha

PISO 6

FAMILIA

Nombre Visitante

Fecha

ADIESTRAMIENTO

FAMILIA

Nombre Visitante

Fecha

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

FAMILIA

REGISTRO DE SALIDAS DE EMPLEADOS

5:00 pm en adelante

Guardián: _____

Puesto: _____

FECHA	NOMBRE EN LETRA DE MOLDE	OFICINA DONDE TRABAJA	HORA DE SALIDA

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

ESTADO LIBRE ASOCIADO DE PUERTO RICO
DEPARTAMENTO DE LA FAMILIA
UNIDAD DE TRANSPORTACION
REGISTRO DE AUTOMOVILES Y CONDUCTORES
AUTORIZADOS A CONDUCIRLOS

FECHA: _____

NOMBRE DEL CONDUCTOR	OFICINA	RUTA	TABLILLA	CANTIDA DE GASOLINA 1.SALIDA 2. ENTRADA	1.HORA 2.MILLAJE DE SALIDA	1.HORA 2.MILLAJE DE ENTRADA	FIRMA DEL CONDUCTOR
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	
				1)	1)	1)	
				2)	2)	2)	

REGISTRO DE GUARDIANES Y TURNOS CORRESPONDIENTES

FIRMA DEL GUARDIAN PRIMER TURNO	HORARIO	FIRMA DEL GUARDIAN SEGUNDO TURNO	HORAIO	FIRMA DEL GUARDIAN TERCER TURNO	HORARIO	COMENTARIO

DEPARTAMENTO FAMILIA
ADFAN ADSEN ADSEF ASUME
Estado Libre Asociado de Puerto Rico

REGISTRO VEHICULAR DE VISITANTES

Departamento de la Familia
Oficina de Manejo de Emergencias y Seguridad

Fecha	Nombre en letra de molde	HORA	Oficina a Visitar	Propósito de la Visita	Número de Tablilla	Marca Vehículo	PISO

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

DEPARTAMENTO FAMILIA
ADFAN ADSEN ADSEF ASUME
Estado Libre Asociado de Puerto Rico

DEFAM-440
SP-02/08

Estado Libre Asociado de Puerto Rico
DEPARTAMENTO DE LA FAMILIA
División de Seguridad y Vigilancia

☐ Secretariado
☐ Administración: _____

INFORME DE INCIDENTES
(Ver instrucciones al dorso)

1. Nombre de la persona o área perjudicada:

2. Grupo al que pertenece: ☐ Empleado(a) ☐ Visitante ☐ Área de trabajo

3. Si es **empleado(a)**, provea la siguiente información:
Puesto que ocupa: _____
Oficina donde trabaja: _____ Teléfono: _____
Si es **visitante**, provea la siguiente información:
Dirección Postal: _____
Teléfono: _____ Otro: _____

4. Fecha del incidente:	5. Hora del incidente:	6. Lugar del incidente:

7. Tipo de incidente:
☐ Vandalismo ☐ Escalamiento ☐ Robo ☐ Fuego ☐ Caída
☐ Otro: _____

8. Persona(s) Testigo(s):		☐ Empleado(a) ☐ Visitante
		☐ Empleado(a) ☐ Visitante

9. Describa brevemente el incidente. De necesitar más espacio, puede utilizar una hoja de papel y graparla a este formulario.

10. Algún otro comentario respecto al incidente:

11. _____ _____
Nombre y firma de persona perjudicada — Fecha

12. _____ _____
Nombre y firma del(de la) Guardia de Seguridad — Fecha

13. _____ _____
Nombre y firma del(de la) Supervisor(a) de Seguridad y Vigilancia — Fecha

Período de Retención: Dos (2) años, previa autorización del(de la) Supervisor(a) de Seguridad y Vigilancia.

ensis SECURITY SERVICES INC.	REPORTE DIARIO	RH-F-24-A PAG 1 DE 1

NOMBRE DE EMPELADO: _____ NUM. EMP.: _____

FECHA: _____ PUESTO: _____

FIRMA DEL OFICIAL: _____ FIRMA SUPERVISOR: _____

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

NOMBRE: _____

FIRMA: _____

PUESTO: _____

FECHA: _____

ASISTENCIA DIARIA

A= ARMADO

D= DESARMADO

FECHA	TOTAL HORAS	NOMBRE EMPLEADO	A/D	TURNO		#EMP	FIRMA EMPLEADO	SUP
				ENTRADA	SALIDA			
LUN___								
T.Hrs___								
MAR___								
T.Hrs___								
MIE___								
T.Hrs___								
JUE___								
T.Hrs___								
VIE___								
T.Hrs___								
SAB___								
T.Hrs___								
DOM___								
T.Hrs___								

HRS A: _____ HRS D: _____ TOTAL HRS: _____

FIRMA DEL SUPERVISOR

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

11 de mayo de 2015

A Todo el Personal de Seguridad
Caseta Italia
Caseta Barbosa

Carmen M. Agosto Serrano
Directora

PROCEDIMIENTOS A SEGUIR SEGÚN SE ESTABLECE EN EL MANUAL DE DIRECTRICES DE SEGURIDAD EN DEPARTAMENTO DE LA FAMILIA EDIFICIO LILA MAYORAL

Con el propósito de garantizar la seguridad de los empleados(as), visitantes, propiedad, planta física y estacionamiento del edificio, se imparten las siguientes directrices:

a. Todo visitante será recibido de forma cortés y atendido con respeto.

b. El guardia de la seguridad privada que se ubica en la caseta Italia estará a cargo del registro vehicular de todo visitante que utilice esa entrada y del registro de empleados autorizados a utilizar vehículos del Departamento para salidas oficiales.

c. El guardia de la seguridad privada que se ubica en la caseta Barbosa estará a cargo del registro vehicular de todo visitante que utilice esa entrada.

d. El personal asignado a ambas casetas utilizará los formularios "*Registro Vehicular de Visitantes*" y "*Registro de Automóviles y Conductores Autorizados a Conducirlos*". (Se ilustra documentos en referencia))
   1) **Registro Vehicular de Visitantes**

   2) **Registro de Automóviles y Conductores Autorizados a Conducirlos**

e. De igual modo, se registran los guardias de la seguridad privada en turnos en la hoja provista por la Compañía contratada identificada como Asistencia Diaria y codificada ADM-F-20-A9 A(Se ilustra el documento en referencia)

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

f. El guardia de la seguridad privada asignado a la ronda y otras áreas del edificio, incluyendo la seguridad de la Unidad de Investigaciones Especiales (UIE), estará en vigilancia continua y deberá notificar a través de sus radios transmisores cualquier situación e incidente que requiera la debida intervención del personal de la Oficina de Seguridad y Manejo de Emergencias, de la Oficina del Secretario Auxiliar de Administración, de la Oficina de la Secretaria o de la Oficina de la Subsecretaria.

g. El personal de la seguridad privada que atienda cualquier hecho suscitado dentro de las facilidades del edificio, estacionamiento, área de la UIE, alrededores del edificio; incluyendo situaciones de protesta, accidentes, hurtos o cualquier otra circunstancia presentada por empleados(as) y visitantes preparará un informe escrito el mismo día del incidente, para lo cual utilizará el formulario *"Informe de Incidencias"*, documento interno que utiliza la compañía de seguridad Privada (Se ilustra documento en referencia).

   Una vez realizado el informe deberá tramitarlo a su supervisor(a) inmediato(a), quien radicará cualquier otro informe, de ser necesario, y entregará los documentos el mismo día del incidente a la Oficina de Seguridad y Manejo de Emergencias.

h. En caso de robo, vandalismo, escalamiento, accidentes, caídas o algún tipo de accidente o situación de riesgo, peligro, daño o pérdidas en las que resulte perjudicado un(a) visitante, un(a) empleada o algún área de trabajo dentro de las facilidades o sus alrededores, incluyendo el estacionamiento; el personal de la Oficina de Seguridad y Vigilancia del Secretariado debe personarse al lugar de los hechos y una vez controlada la situación debe completar el formulario *"Informe de Incidentes"*, DEFAM-440(Se ilustra documento en referencia. Este informe se realiza en presencia de las partes involucradas; y en casos, cuando es el resultado de pérdidas, en presencia del personal de seguridad privada y de testigos, de haber alguno.

i. El DEFAM-440, *Informe de Incidentes*, también deberá ser utilizado en situaciones de protesta y manifestaciones presentadas en los alrededores, siempre y cuando el personal de seguridad, entiéndase guardias y personal de la Oficina de Seguridad y Vigilancia del Departamento, intervengan con el o los manifestantes. En el informe se detallará el hecho suscitado, la intervención, el manejo del asunto, los resultados y/o cualquier directriz o acción tomada ante la eventualidad.

Cualquier situación presentada fuera de horas laborables será manejada por el personal de seguridad privada, incluido el guardia asignado a la UIE. El guardia de la seguridad privada informará al personal de la Oficina de Seguridad y Manejo de Emergencia sobre la situación y manejará la situación hasta que el personal de la Oficina de Seguridad y Manejo de Emergencia o quien se determine intervendrá con la situación se presente al edificio.

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

11 de mayo de 2015

PERSONAL DE RECEPCIÓN

Carmen M. Agosto Serrano
Directora

PROCEDIMIENTOS PARA LA ATENCION DE VISITANTES Y EMPLEADOS SEGÚN SE ESTABLECE EN EL MANUAL DE DIRECTRICES DE SEGURIDAD DEL DEPARTAMENTO DE LA FAMILIA EDIFICIO LILA MAYORAL

Con el propósito de garantizar la seguridad de los empleados(as) y visitantes, se imparten las siguientes directrices para la atención y manejo al personal de recepción del departamento:

a. La (El) recepcionista o cualquier otro personal que la sustituya, atenderá la recepción principal del Departamento de forma cortés y con el respeto que merece todo(a) empleado(a) y visitante que acuda a nuestra dependencia diariamente.

b. La (El) recepcionista solicitará una identificación con foto válida a toda persona que solicite autorización para entrar al edificio en busca de recibir o dar servicios, acudir a cita o reunión, entregar documentos o cualquier otro asunto.

c. La (El) recepcionista deberá anotar la información de todo visitante en el formulario *"Registro de Visitas Diarias" (Se ilustra documento en referencia),* con excepción de aquellos que visitarán los salones de adiestramiento.

d. La (El) recepcionista le proveerá una pegatina a cada visitante, la cual será impresa en siete colores diferentes. Cada piso estará identificado con un color y los salones de adiestramiento. Esta pegatina ayudará al personal de seguridad y empleados(as) a identificar visitantes no autorizados a otras áreas.

e. Toda persona que requiera visitar la Oficina de la Secretaria, Subsecretaria, División Legal, Secretaria Auxiliar de Planificación, Oficina de Prensa al igual que la Oficina de la Administradora de la ADFAN, deberá ser anunciada a la oficina indicada para autorización de acceso al área solicitada.

Oficina de Seguridad y Manejo de Emergencias
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.294.4900 Fax: 787.294.0732

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

f. Cualquier situación referente a visitantes sospechosos deberá ser notificada al personal de seguridad privada y a la Oficina de Seguridad y Manejo de Emergencias. La notificación deberá ser realizada a través de los radios comunicadores o a través del cuadro telefónico, según lo amerite la circunstancia.

g. Cuando la (el) recepcionista entienda que requiere de la presencia del personal de seguridad privada o la escolta de cualquier visitante a oficinas, deberá solicitarlo inmediatamente y notificar a la Oficina de Seguridad y Manejo de Emergencias sobre la situación.

h. Todo empleado que labore en el edificio deberá tener accesible su identificación para propósitos de facilitar la identificación del personal autorizado a entrar al edificio sin la debida registración requerida.

i. Toda persona visitante que acuda a nuestro edificio para tomar talleres o adiestramientos programados deberá ser orientado por la (el) recepcionista o por un ujier de haber sido establecido el mismo sobre la ubicación del lugar a visitar.

j. El personal encargado del taller y/o adiestramiento será responsable de entregar copia de la "Hoja de Asistencia" en la recepción una vez finalizado el taller para propósitos del registro diario de visitantes del edificio.

k. Todo(a) empleado(a) que abandone el edificio posterior a su horario regular de salida debe firmar el registro de salidas de empleados 5:00pm en adelante (Se ilustra documento en referencia) ubicado en la recepción. (Esto no aplica a personal de confianza)

l. El personal de Seguridad y Recepción debe asegurarse que toda solicitud para acceso al edificio fuera de horas laborales este debidamente autorizada por la Oficina de Seguridad y Manejo de Emergencias. Esto incluye acceso para fines de semanas y días feriados.

APÉNDICE 2

REGISTRO DE VISITANTES AL ÁREA COMÚN DEL DATA CENTER DE LA OSI

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

REGISTRO DE VISITANTES AL ÁREA COMÚN DEL *DATA CENTER* EN LA OFICINA DE SISTEMAS DE INFORMACIÓN

Fecha	Hora de Entrada	Hora de Salida	Nombre y Apellidos (Use letra de molde) y Firma	Compañía	Razón de Visita	Observaciones

Oficina de Sistemas de Información
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.625.4900 Exts.: 1008 y 1073

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

APÉNDICE 3

REGISTRO DE VISITANTES AL ÁREA ADMINISTRATIVA DE LA OSI

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

REGISTRO DE VISITANTES AL ÁREA ADMINISTRATIVA DE LA OFICINA DE SISTEMAS DE INFORMACIÓN

Fecha	Hora de Entrada	Hora de Salida	Nombre y Apellidos (Use letra de molde) y Firma	Compañía	Razón de Visita	Observaciones

Oficina de Sistemas de Información
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.625.4900 Exts.: 1008 y 1073

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

APÉNDICE 4

COMUNICACIÓN CONTROL DE ACCESO AL ÁREA DE OPERACIONES DE LA OSI

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

6 de julio de 2015

A Todo El Personal de la Oficina de Sistemas de Información

PROCEDIMIENTO CONTROL DE ACCESO AL AREA OPERACIONAL DE LA OFICINA DE SISTEMAS DE INFORMACIÓN

La naturaleza de nuestra oficina requiere que la seguridad sea atendida **con todo rigor.** Somos responsables del Centro de Cómputos que da servicio a los empleados en la prestación de sus labores diarias como usuarios de los sistemas mecanizados. El personal de la Oficina de Sistema de información cuenta con tarjeta electrónica de acceso para acceder a su área de trabajo. Como medida de control se implanta la siguiente directriz a seguir:

1. **Acceso al área común de la Oficina de Sistemas de Información**

   Toda persona que tenga que entrar a ejercer funciones oficiales y no sea empleado de la Oficina de Sistemas de Información, deberá llenar la información solicitada en el Registro de Acceso: deberá llenar la información indicada como su nombre, hora de entrada, hora de salida, razón de visita y firma (anejo-1). Este registro incluye a todos los empleados que vengan en calidad de usuarios del sistema o a brindarnos servicios de limpieza, mensajería entre otros.

2. **Acceso al área restringida del Data Center**

   Solo el personal debidamente autorizado podrá tener acceso al área. Cualquier otra persona deberá solicitar autorización del área al supervisor antes de su acceso y completar la información solicitada en la Bitácora o Registro de acceso al centro de cómputos como: nombre, hora de entrada, hora de salida, razón, firma del visitante y del supervisor que autorizo acceso (anejo-2).

   Esto incluye a todos los empleados que vengan en calidad de usuarios del Sistema o a brindarnos servicios de apoyo a servidores, mantenimiento de aires, mensajería, limpieza y otros. El código de acceder al Data Center solo lo tienen las personas autorizadas como parte de sus funciones acceder a esta área.

Oficina de la Sistemas de Información
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.721-4747

3. **Personal no autorizado**

   Queda terminantemente prohibido a todo personal que no esté en Funciones Oficiales, permanecer en la Oficina de Sistemas de Información.

Con estas medidas y por seguridad, se salvaguarda la propiedad y los documentos de la Oficina.

De manera inmediata será establecido el nuevo procedimiento de acceso al área de operaciones de la Oficina de Sistemas de Información del Secretariado del Departamento de la Familia.

Cordialmente,

Víctor R. Burgos

Víctor R. Burgos, Director
Oficina de Sistemas de Información
vburgos@familia.pr.gov
Tel. (787)294-4900 ext. 1185

APÉNDICE 5

REGISTRO DE VISITANTES AL DATA CENTER

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

REGISTRO DE VISITANTES AL *DATA CENTER*

Fecha	Hora de Entrada	Hora de Salida	Nombre y Apellidos (Use letra de molde) y Firma	Compañía	Razón de Visita	Firma de Persona que Autorizó Visita Nombre y Apellidos (Use Letra de Molde)

Oficina de Sistemas de Información
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.625.4900 Exts.: 1008 y 1073

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

APÉNDICE 6

CONTROL DE USO DE LLAVES CUARTOS DE COMUNICACIÓN - OSI

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

CONTROL DE USO DE LLAVES CUARTOS DE COMUNICACIÓN - OSI

NOMBRE	FECHA Y HORA DE ENTREGA	NÚM. LLAVE	FECHA Y HORA DE DEVOLUCIÓN	FIRMA

Oficina de Sistemas de Información
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.625.4900 Exts.: 1008 y 1073

APÉNDICE 7

DESIGNACIÓN DE USUARIOS CUENTAS ADMINISTRADOR DE DOMINIOS

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

22 de febrero de 2016

Miguel Hernández Torres
Supervisor Área Operaciones
Oficina Sistemas de Información
Secretariado

Blanca Pérez Torres
Directora
Oficina Sistemas de Información

DESIGNACION DE USUARIOS CUENTAS ADMINISTRADOR DE DOMINIOS

Conforme se desprende de los documentos históricos existentes en esta Oficina las personas designadas como Administradores de Dominio por el pasado Director son el Sr. Miguel Hernández Torres y el Sr. Howard Hatchett Ortiz. Mediante esta comunicación confirmo que prevalece la directriz dada por el pasado Director. Igualmente estoy designando al Sr. Jose Flores, Supervisor de Procesamiento de Datos, para que sea añadido al grupo de Administradores de Dominio.

Agradeceré imparta las directrices correspondientes para que este grupo quede constituido en los sistemas conforme autorizado. De requerir información adicional no dude en contactarnos.

Acuse de Recibo

Miguel Hernández Torres

22-febrero-2016
Fecha

Cf. José Flores – Supervisor Procesamiento de Datos
Howard Hatchett – Técnico de Redes

APÉNDICE 8

DEFAM-516

SOLICITUD DE ACCESO A LOS SISTEMAS

DEFAM-516
SP 05/2014
Antes (OSI-01-09)

Estado Libre Asociado de Puerto Rico
DEPARTAMENTO DE LA FAMILIA
Oficina Sistemas de Información

Período de Retención:
Un (1) año después que el empleado se desvincule del Departamento de la Familia.

Componente Operacional

☐ Secretariado _____ ☐ Región: _____

☐ Administración: _____ ☐ Local: _____

SOLICITUD DE ACCESO A LOS SISTEMAS

A. SOLICITUD

I. Información del Solicitante

a. Nombre, Inicial, Apellidos: _____

b. Números Telefónicos: _____

II. Accesos y Acción

Acceso	Acción			Comentarios
	Activar	Desactivar	Modificar	
☐ Cuenta[1]				
☐ Correo Electrónico				
☐ Internet[2]				
☐ Aplicaciones Especiales[3]				
☐ Remoto				
☐ PRIFAS				
☐ RHUM				

III. Acuerdo

Al firmar este documento reconozco que soy responsable por la cuenta creada en el sistema y los accesos autorizados. Cualquier mal uso de la cuenta dentro del sistema, podría conllevar sanciones, y de ser necesario, la suspensión de los servicios recibidos.

Firma del Usuario: _____ Fecha _____

IV. Autorización del Supervisor

Certifico que _____ requiere de los accesos solicitados para llevar a cabo sus labores, por lo que esta solicitud cuenta con mi autorización.

Nombre y Firma del Supervisor: _____ Fecha: _____

B. ACCIÓN TOMADA (Para uso de la Oficina de Sistemas de Información-Área de Seguridad)

Certifico que se evaluó la solicitud del(de la) empleado(a) y se tomó la siguiente determinación:

☐ Se dio(eron) los accesos solicitados.

☐ Se asignó contraseña provisional para acceder.

Nombre del Usuario: _____

Contraseña Asignada: _____

Comentarios: _____

_____

_____ _____
Nombre y Firma del(de la) Representante Autorizado(a) Fecha

[1] La División de Seguridad de la Oficina de Sistemas de Información revisará periódicamente la utilización de las cuentas y desactivará aquellas que no han sido usadas en 90 días o más. De esto suceder, el usuario tendrá que gestionar la activación de la cuenta nuevamente.

[2] Toda persona que solicite acceso a la Internet tiene que completar el formulario DEFAM-517,"Solicitud y Autorización para Acceso a la Internet" y carta de justificación.

[3] Se consideran aplicaciones especiales las diseñadas para propósitos específicos, tales como: SAIC, EBT, SADE, CeSI, entre otros. Debe completar el formulario "Solicitud de Acceso a Aplicaciones Especiales", del componente al que está adscrito (DEFAM-518, ACUDEN; DEFAM-519, ADFAN; DEFAM-520, ADSEF).

DESCRIPCIÓN

El formulario DEFAM-516, "Solicitud de Acceso a los Sistemas", lo utiliza el empleado para solicitar acceso a cuenta de usuario, correo electrónico, internet, entre otros. El personal de la Oficina de Sistemas de Información evalúa y autoriza o deniega el acceso a los sistemas.

INSTRUCCIONES

Complete cada una de las partes de este formulario. Si alguna no aplica, debe indicar N/A.

En el inicio del formulario, seleccione el componente operacional al que pertenece el solicitante y la oficina en donde trabaja.

A. SOLICITUD

I. **Información del Solicitante –** El solicitante debe anotar su nombre, inicial y los dos apellidos, sus números telefónicos y el "user name", si previamente fue asignado.

II. **Acceso y Acción –** En esta área el solicitante indicará el acceso que solicita y la acción a tomarse. Además, puede incluir cualquier comentario que entienda necesario. En el caso del acceso a aplicaciones especiales, debe anotar los nombres de las aplicaciones que solicita en el encasillado de comentarios.

III. **Acuerdo –** Con su firma, el solicitante certifica que leyó y conoce la norma relacionada a este asunto. Además, anotará la fecha del día que lo completa.

IV. **Visto Bueno del Supervisor –** El Supervisor firma y certifica con su visto bueno lo solicitado por el solicitante.

B. AUTORIZACIÓN (Sólo para uso de la Oficina de Sistemas de Información) – El Oficial de Seguridad certifica que evaluó la solicitud e informa la determinación. Si la solicitud es denegada, debe indicar la razón. Además, se provee espacio para cualquier otro comentario que estime conveniente.

POLÍTICA DE CONFIDENCIALIDAD – Toda la información contenida en el sistema es confidencial, privilegiada y/o privada bajo la ley aplicable; y se utilizará solamente para brindar servicios. Se prohíbe estrictamente la divulgación de información contenida en el sistema y la utilización de este sistema para un uso distinto al estipulado.

La política pública del Departamento de la Familia prohíbe el discrimen de clase alguna, entre otros motivos, por género. Por lo tanto, para propósitos de este documento, todo término que se utilice al mencionar una persona o puesto se refiere a ambos géneros.

Toda solicitud de corrección, revisión o derogación de este formulario debe ser tramitada a la Oficina de Sistemas y Procedimientos.

Mayo 2014

APÉNDICE 9

DEFAM-517

SOLICITUD DE ACCESO A LA INTERNET

DEFAM-517
SP 05/2014
Antes (OSI-01-09)

Estado Libre Asociado de Puerto Rico
DEPARTAMENTO DE LA FAMILIA
Oficina Sistemas de Información

Período de Retención: Disponer de un (1) año después que el empleado se desvincule del Departamento de la Familia.

SOLICITUD DE ACCESO A LA INTERNET

A. SOLICITUD

I. INFORMACIÓN DEL USUARIO

a. Nombre, Inicial, Apellidos: _____

b. Clasificación: _____

c. Números Telefónicos: _____

d. Ubicación: (Secretariado, ADFAN, ACUDEN) _____

II. DESCRIPCIÓN DEL TRABAJO A REALIZARSE A TRAVÉS DE LA INTERNET

_____

_____

III. DIRECTRICES SOBRE EL USO CORRECTO DE LA INTERNET

Este servicio está restringido al uso **con carácter oficial relacionado con la labor que realiza el empleado en la Agencia**. Cualquier uso distinto al establecido constituye uso indebido del mismo. Los usos no aceptables incluyen, pero no se limitan a:

a) **Uso para actividades de lucro:** Uso de los equipos de la agencia para actividades de lucro (trabajo de consultoría con paga, compra o venta de productos, negocios primados o personales, juegos de azar, etc.

b) **Impacto Negativo:** La utilización del Internet para actividades que influencian, afectan o van en detrimento de la imagen de cualquier persona, organización o del Estado Libre Asociado de Puerto Rico está terminantemente prohibido.

c) **Manejo de Archivos Voluminosos:** La transferencia de archivos voluminosos a los sistemas de la Agencia está terminantemente prohibido. Esto incluye música o videos de cualquier tipo de formato.

d) **Actos Maliciosos:** Propagación de virus, material ofensivo o pornográfico. Actos ilegales y en detrimento al funcionamiento de los sistemas y a la imagen de la Agencia.

IV. ACEPTACIÓN DE CONDICIONES

Certifico entender y estar de acuerdo con lo expuesto en este documento referente a la correcta utilización del Internet.

_____ _____
Firma del Empleado Fecha

V. AUTORIZACIÓN DEL SUPERVISOR

Certifico que el empleado objeto de esta solicitud, requiere el uso de Internet para llevar a cabo sus labores; por tal razón, cuenta con mi autorización.

_____ _____
Nombre y Firma del Supervisor Fecha

B. ACCIÓN TOMADA (Para uso de la Oficina de Sistemas de Información)

Certifico que evalué esta solicitud y la misma fue: ☐ Aprobada ☐ Denegada, Razón: _____

_____

Se autorizó el siguiente grupo de usuarios: ☐ Regulares ☐ Consultores ☐ Gerenciales
☐ Gerenciales *Medium Access* ☐ Gerenciales *Full Access*

Nombre y Firma del Oficial de Seguridad: _____ Fecha: _____

DESCRIPCIÓN

El formulario DEFAM-517, "Solicitud de Acceso a la Internet", lo utiliza la Oficina de Sistemas de Información para autorizar el acceso a la Internet a los empleados del Departamento de la Familia.

INSTRUCCIONES

Complete cada una de las partes de este formulario. Si alguna no aplica, debe indicar N/A.

A. SOLICITUD

I. **Información del Usuario** – El usuario debe anotar el nombre, inicial y apellidos, clasificación, números telefónicos e indicar la ubicación en la Administración donde trabaja.

II. **Descripción del Trabajo a Realizarse a Través de la Internet** – En esta área el usuario describe brevemente el trabajo que realiza y el acceso que necesita para realizar sus funciones.

III. **Directrices sobre el Uso Correcto de la Internet** – En esta área se detallan las restricciones en el uso del Internet.

IV. **Aceptación de Condiciones** – El usuario certifica que entendió las condiciones y que utilizará correctamente el Internet.

V. **Certificación del Supervisor** – El Supervisor del usuario certifica que este necesita hacer uso del Internet.

B. ACCIÓN TOMADA

El Oficial de Seguridad certifica que evaluó la solicitud e informa la determinación. Si la solicitud es denegada, debe indicar la razón. Una vez autorizada, indica el grupo de usuario asignado:

- Usuarios Regulares – Acceso limitado a páginas autorizadas.
- Usuarios Consultores – "Solo existe en dominio DLF". Acceso al Internet con limitaciones a *downloads* y páginas de información.
- Usuarios Gerenciales – Usuarios con acceso a todas las páginas en excepción a *social network*, *media streaming* y *news and media*.
- Usuarios Gerenciales *Medium Access* – Usuarios con acceso a todas las páginas en excepción a *social network* y *media streaming*.
- Usuarios Gerenciales *Full Access* – Usuarios con acceso a todas las páginas.

La política pública del Departamento de la Familia prohíbe el discrimen de clase alguna, entre otros motivos, por género. Por lo tanto, para propósitos de este documento, todo término que se utilice al mencionar una persona o puesto se refiere a ambos géneros.

Toda solicitud de corrección, revisión o derogación de este formulario debe ser tramitada a la Oficina de Sistemas y Procedimientos.

Mayo 2014

APÉNDICE 10

DEFAM-518

SOLICITUD DE ACCESO A APLICACIONES ESPECIALES – ACUDEN

Estado Libre Asociado de Puerto Rico
Departamento de la Familia
Oficina de Sistemas de Información

Periodo de Retención:

Un año luego de que el empleado se desvincule del Departamento de la Familia.

SOLICITUD DE ACCESO A APLICACIONES ESPECIALES - ACUDEN

I. Información del Usuario:

Nombre: _____ Segundo Nombre: _____

Apellidos: _____

Clasificación: _____

Núm. Tel. Oficina: _____ Correo Electrónico: _____

Ubicación: ☐ Central ☐ Regional ☐ Agencia Delegada ☐ Centro Cuido

Oficina (Especifique): _____

Cuenta de Usuario: _____

II. Aplicaciones Especiales:

A. Sistema CIMA – Manejo de Casos - *Child Care*

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Proveedores ☐ Administración y Seguridad
☐ Certificación de Asistencias ☐ Pagos ☐ Reportes

Privilegios: ☐ Añadir Transacciones ☐ Modificar Transacciones ☐ Consulta

Puesto Funcional: ☐ Director(a) ☐ Coordinador(a) Auxiliar ☐ Técnico(a) de Familias
☐ Técnico(a) de Proveedores ☐ Control de Calidad ☐ Data Entry (801)

B. Sistema PROMIS – Manejo Casos – Programa Head Start

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Alianza ☐ Salud Médico/Dental ☐ Necesidades Especiales ☐ Educación
☐ Salud Mental ☐ Recursos Humanos

Privilegios: ☐ Añadir Transacciones ☐ Modificar Transacciones ☐ Consulta

Puesto Funcional: ☐ Director(a) ☐ Subdirector(a) ☐ Gerente ☐ Supervisor(a) ☐ Coordinador(a)
☐ Trabajador(a) Social ☐ Data Entry ☐ Maestro(a) ☐ Técnico(a) de Servicios
☐ Administrador(a) Sistema ACUDEN ☐ Administrador(a) Sistema Agencia Delegada

C. Sistema MIP – Manejo de Presupuesto y Contabilidad - Áreas Fiscales

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Obligaciones ☐ Cuentas por Cobrar ☐ Administración y Seguridad
☐ Cuentas a Pagar ☐ Presupuesto ☐ Reportes

Privilegios: ☐ Añadir Transacciones ☐ Modificar Transacciones ☐ Consulta

Puesto Funcional: ☐ Director(a) ☐ Subdirector(a) ☐ Gerente ☐ Supervisor(a) ☐ Coordinador(a)
☐ Trabajador(a) Social ☐ Contador(a) ☐ Auxiliar de Contabilidad
☐ Técnico(a) de Servicios ☐ Técnico(a) de Presupuesto

D. Sistema FAS-GOV – Manejo de Activo Fijo – Nivel Central

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Manejo de Inventario ☐ Contabilidad ☐ Disposición de Activos
☐ Administración y Seguridad ☐ Reportes

Privilegios: ☐ Añadir Transacciones ☐ Modificar Transacciones ☐ Consulta

Puesto Funcional: ☐ Director(a) ☐ Supervisor(a) ☐ Técnico(a) de Propiedad

E. Sistema E-ROC – Requisiciones de Compra – Nivel Central

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Procesos de Requisición ☐ Procesos de Aprobación ☐ Procesos de Compra
☐ Procesos de Autorización ☐ Procesos de Posteo a MIP ☐ Administración y Seguridad

Privilegios: ☐ Añadir Transacciones ☐ Modificar Transacciones ☐ Consulta

Puesto Funcional: ☐ Administrador(a) ☐ Administrador(a) Auxiliar ☐ Director(a) ☐ Subdirector(a)
☐ Supervisor(a) ☐ Contador(a) ☐ Técnico(a) de Presupuesto ☐ Secretaria(a) ☐ Oficinista

III. Acuerdo

Al firmar este documento, reconozco que soy responsable por la cuenta creada en el sistema a mi nombre. Además, certifico que he leído y me comprometo a cumplir con las normas y procedimientos establecidos en el "Manual de Normas sobre el Uso de Tecnologías de la Información". Entiendo que cualquier mal uso de la cuenta y accesos autorizados podría conllevar medidas disciplinarias establecidas en la reglamentación vigente del Departamento.

_____ _____

Firma del(de la) Empleado(a) Fecha

IV. Política de Confidencialidad

Toda la información contenida en el sistema es confidencial, privilegiada y privada bajo la ley aplicable. La información se utilizará solamente para brindar servicios a los individuos o participantes del Departamento. Se prohíbe estrictamente la divulgación de información contenida en los sistemas a los cuales se le proveerá acceso.

_____ _____

Firma del(de la) Empleado(a) Fecha

V. Autorización del Supervisor

Certifico que este(a) empleado(a) requiere de las aplicaciones especiales antes solicitadas para llevar a cabo sus labores, por lo que esta solicitud cuenta con mi autorización.

_____ _____

Nombre y Firma del(de la) Supervisor(a) Fecha

▼PARA SER COMPLETADO POR LA OFICINA DE SISTEMAS DE INFORMACIÓN▼

VI. Acción Tomada

Certifico que se evalúo la solicitud del(de la) empleado(a) y se tomó la siguiente determinación:

☐ Se dio(eron) el(los) acceso(s) solicitado(s).

☐ Se dio(eron) el(los) acceso(s) solicitado(s), excepto: _____

Razón: _____

☐ Se asignó contraseña provisional para acceder.

Nombre de(de la) Usuario: _____

Contraseña Asignada[1]: _____

Comentarios: _____

_____ _____

Nombre y Firma del(de la) Representante Autorizado(a) Fecha

[1]El sistema formazará al usuario a cambiar esta contraseña la privera vez que la utilice.

DESCRIPCIÓN

El formulario DEFAM-518, "Solicitud de Acceso a Aplicaciones Especiales – ACUDEN", lo utiliza el personal de la Administración para el Cuidado y Desarrollo Integral de la Niñez (ACUDEN) para solicitar al personal de la Oficina de Sistemas de Información acceso a aplicaciones especiales; quienes a la vez, evalúan y dan el(los) acceso(s) solicitado(s).

INSTRUCCIONES GENERALES

Lea las siguientes instrucciones y complete cada una de las partes del formulario. Si algún encasillado no aplica, favor de escribir N/A.

I. Información del(de la) Usuario – Anote el nombre del(de la) usuario, clasificación, número telefónico de la oficina, correo electrónico, ubicación, oficina en que labora y cuenta de usuario.

II. Aplicaciones Especiales – Seleccione las aplicaciones para las cuales solicita activación, desactivación o modificación. Además, indique el tipo de acceso, privilegio y puesto funcional. Si alguna no aplica, seleccione la alternativa provista para tal propósito en cada aplicación.

III. Política de Confidencialidad – Lea la política y certifique tal acciones estampando sus iniciales y fecha en el espacio provisto.

IV. Acuerdo – Lea el acuerdo que conlleva la aprobación de aplicaciones especiales y certifique con su firma, y anote la fecha en que llevó a cabo tal acción.

V. Autorización del(de la) Supervisor(a) – En esta parte, el(la) supervisor(a) del(de la) empleado(a) certifica que los accesos a las aplicaciones especiales son necesarios. El(La) supervisor(a) anota su nombre, firma y escribe la fecha en que completó el documento.

VI. Acción Tomada – El(La) representante autorizado(a) certifica que evaluó la solicitud e indica la acción tomada. Además, asigna una contraseña provisional al usuario con la que podrá acceder las aplicaciones especiales; y anota la fecha en que completó el documento.

La política pública del Departamento de la Familia prohíbe el discrimen de clase alguna, entre otros motivos, por género. Por lo tanto, para propósitos de este documento, todo término que se utilice al mencionar una persona o puesto se refiere a ambos géneros.

Toda solicitud de corrección, revisión o derogación de este formulario debe ser tramitada a la Oficina de Sistemas y Procedimientos.

Mayo 2014

APÉNDICE 11

DEFAM-519

SOLICITUD DE ACCESO A APLICACIONES ESPECIALES – ADFAN

Estado Libre Asociado de Puerto Rico
Departamento de la Familia
Oficina de Sistemas de Información

Período de Retención:

Un año luego de que el empleado se desvincule del Departamento de la Familia.

SOLICITUD DE ACCESO A APLICACIONES ESPECIALES - ADFAN

I. Información del Usuario:

Nombre: _____ Segundo Nombre: _____

Apellidos: _____

Clasificación: _____

Núm. Tel. Oficina: _____ Correo Electrónico: _____

Ubicación: ☐ Central ☐ Regional ☐ Agencia Delegada ☐ Centro Cuido

Oficina (Especifique): _____

Cuenta de Usuario: _____

II. Aplicaciones Especiales:

A. Sistema *AFCARS (Legacy) – Adoption and Foster Care Analysis and Report System*

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Internet (actualización anti-virus)

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Director(a) ☐ Coordinador(a) SIS ☐ *Data Entry*
☐ Auxiliar de Sistemas de Oficina ☐ Supervisor(a) Cuidado Sustituto

B. Sistema TÍTULO IV-B (Aplicación)

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Internet

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Director(a) ☐ Coordinador(a) Título IV-E ☐ Trabajador(a) Social
☐ Auxiliar de Sistemas de Oficina ☐ Supervisor(a) Cuidado Sustituto
☐ Técnico(a) de Servicios a la Familia

C. Sistema SICStA

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Internet

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Director(a) ☐ Coordinador(a) SICStA ☐ Trabajador(a) Social
☐ Técnico(a) de Servicios a la Familia ☐ Supervisor(a) Cuidado Sustituto
☐ Supervisor(a) Regional ☐ Supervisor(a) Local

D. Sistema *NCANDS – National Child Abuse and Neglect Data System*

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Internet

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Director(a) ☐ Coordinador(a) ☐ Trabajador(a) Social
☐ Técnico(a) de Servicios a la Familia ☐ Supervisor(a) Cuidado Sustituto
☐ Supervisor Regional ☐ Supervisor Local

E. Sistema SIRCe

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Internet

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Director(a) ☐ Trabajador(a) Social ☐ Técnico(a) de Servicios a la Familia
☐ Supervisor(a) Cuidado Sustituto ☐ Supervisor(a) Regional ☐ Supervisor(a) Local

F. **REVA – Registro Estatal Voluntario de Adopción**

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Internet

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Director(a) ☐ Coordinador de Adopción ☐ Trabajador(a) Social ☐ Técnico(a) de Servicios a la Familia ☐ Supervisor(a) Cuidado Sustituto ☐ Supervisor(a) Regional ☐ Supervisor(a) Local

G. **Control de Llamadas de la Línea de Orientación y Apoyo Familiar**

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ Familias y Niños ☐ Internet

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Director(a) ☐ Coordinador ☐ Trabajador(a) Social ☐ Técnico(a) de Servicios a la Familia ☐ Supervisor(a) Cuidado Sustituto ☐ Supervisor(a) Regional ☐ Supervisor(a) Local

H. **CyberFusion (ADCARS y NYTD) – Transmitir Datos al Gobierno Federal**

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Accesos: ☐ ADFANWUS ☐ Internet

Privilegios: ☐ Añadir Datos ☐ Editar Datos ☐ Informes

Puesto Funcional: ☐ Persona Designada para Transmisión AFCARS ☐ Persona Designada para Transmisión NYTD

III. Acuerdo

Al firmar este documento, reconozco que soy responsable por la cuenta creada en el sistema a mi nombre. Además, certifico que he leído y me comprometo a cumplir con las normas y procedimientos establecidos en el "Manual de Normas sobre el Uso de Tecnologías de la Información". Entiendo que cualquier mal uso de la cuenta y accesos autorizados podría conllevar medidas disciplinarias establecidas en la reglamentación vigente del Departamento.

_____ _____

Firma del(de la) Empleado(a) Fecha

IV. Política de Confidencialidad

Toda la información contenida en el sistema es confidencial, privilegiada y privada bajo la ley aplicable. La información se utilizará solamente para brindar servicios a los individuos o participantes del Departamento. Se prohíbe estrictamente la divulgación de información contenida en los sistemas a los cuales se le proveerá acceso.

_____ _____

Firma del(de la) Empleado(a) Fecha

V. Autorización del Supervisor

Certifico que este(a) empleado(a) requiere de las aplicaciones especiales antes solicitadas para llevar a cabo sus labores, por lo que esta solicitud cuenta con mi autorización.

_____ _____

Nombre y Firma del(de la) Supervisor(a) Fecha

▼PARA SER COMPLETADO POR LA OFICINA DE SISTEMAS DE INFORMACIÓN▼

VI. Acción Tomada

Certifico que se evalúo la solicitud del(de la) empleado(a) y se tomó la siguiente determinación:

☐ Se dio(eron) el(los) acceso(s) solicitado(s).

☐ Se dio(eron) el(los) acceso(s) solicitado(s), excepto: _____

Razón: _____

_____

☐ Se asignó contraseña provisional para acceder.

Nombre de(de la) Usuario: _____

Contraseña Asignada[1]: _____

Comentarios: _____

_____

_____

_____

_____

_____ Nombre y Firma del(de la) Representante Autorizado(a)

_____ Fecha

[1]El sistema formazará al usuario a cambiar esta contraseña la privera vez que la utilice.

DESCRIPCIÓN

El formulario DEFAM-519, "Solicitud de Acceso a Aplicaciones Especiales – ADFAN", lo utiliza el personal de la Administración de Familias y Niños (ADFAN) para solicitar al personal de la Oficina de Sistemas de Información acceso a aplicaciones especiales; quienes a la vez, evalúan y dan el(los) acceso(s) solicitado(s).

INSTRUCCIONES GENERALES

Lea las siguientes instrucciones y complete cada una de las partes del formulario. Si algún encasillado no aplica, favor de escribir N/A.

I. Información del(de la) Usuario – Anote el nombre del(de la) usuario, clasificación, número telefónico de la oficina, correo electrónico, ubicación, oficina en que labora y cuenta de usuario.

II. Aplicaciones Especiales – Seleccione las aplicaciones para las cuales solicita activación, desactivación o modificación. Además, indique el tipo de acceso, privilegio y puesto funcional. Si alguna no aplica, seleccione la alternativa provista para tal propósito en cada aplicación.

III. Política de Confidencialidad – Lea la política y certifique tal acciones estampando sus iniciales y fecha en el espacio provisto.

IV. Acuerdo – Lea el acuerdo que conlleva la aprobación de aplicaciones especiales y certifique con su firma, y anote la fecha en que llevó a cabo tal acción.

V. Autorización del(de la) Supervisor(a) – En esta parte, el(la) supervisor(a) del(de la) empleado(a) certifica que los accesos a las aplicaciones especiales son necesarios. El(La) supervisor(a) anota su nombre, firma y escribe la fecha en que completó el documento.

VI. Acción Tomada – El(La) representante autorizado(a) certifica que evaluó la solicitud e indica la acción tomada. Además, asigna una contraseña provisional al usuario con la que podrá acceder las aplicaciones especiales; y anota la fecha en que completó el documento.

La Oficina de Sistemas de Información informará mediante correo electrónico la acción tomada (a la) director(a) de la oficina solicitante y al(a la) supervisor(a) del(de la) empleado(a) solicitante.

La política pública del Departamento de la Familia prohíbe el discrimen de clase alguna, entre otros motivos, por género. Por lo tanto, para propósitos de este documento, todo término que se utilice al mencionar una persona o puesto se refiere a ambos géneros.

Toda solicitud de corrección, revisión o derogación de este formulario debe ser tramitada a la Oficina de Sistemas y Procedimientos.

Mayo 2014

APÉNDICE 12

DEFAM-520

SOLICITUD DE ACCESO A APLICACIONES ESPECIALES – ADSEF

Estado Libre Asociado de Puerto Rico
Departamento de la Familia
Oficina de Sistemas de Información

Período de Retención:

Un año luego de que el empleado se desvincule del Departamento de la Familia.

Solicitud de Acceso a Aplicaciones Especiales - ADSEF

I. Información del Usuario:

Nombre: _____ Segundo Nombre: _____
Apellidos: _____
Clasificación: _____
Núm. Tel. Oficina: _____ Correo Electrónico: _____
Ubicación: ☐ Central ☐ Regional ☐ Agencia Delegada ☐ Centro Cuido
Oficina (Especifique): _____
Cuenta de Usuario: _____

II. Aplicaciones Especiales:

A. Sistemas:

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios

Accesos: ☐ SAICWEB ☐ SIBFAM ☐ HOGARES ☐ PROVMS ☐ SIBIF ☐ SADE ☐ QAVMS
☐ DESEMPLEO Y SALUD ☐ DEVSAIC (TRAINING) ☐ KRONOS ☐ SISMAC ☐ QUANIX
☐ CIMA ☐ INTERNET ☐ EBT ☐ CALENDARIO

B. Sistema de Administración e Información de Casos (SAIC y EBT)

Acción: ☐ Activar Usuario ☐ Desactivar Usuario ☐ Modificar Privilegios ☐ No Aplica

Puesto Funcional: ☐ Director(a) ☐ Supervisor(a) ☐ Oficinista ☐ Ofic. Reclamaciones Sustituto
☐ Supervisor(a) de Manejador ☐ Oficinista de Reclamaciones
☐ Pagador(a) Sustituto ☐ Oficial PAN y TRABAJO ☐ Recaudador Sustituto
☐ Pagador(a) ☐ Técnico(a) ☐ Recaudador(a) ☐ Oficinista Recepción
☐ Manejador(a) ☐ Otro

Grupo Asignado: (Escoja sólo uno.) ☐ Director(a) ☐ Supervisor(a) ☐ "Help Desk" ☐ Operaciones ☐ Apoyo Técnico
☐ Telecomunicaciones ☐ Control de Calidad ☐ Técnico(a) de Seguridad
☐ Oficinista/Recepción ☐ Análisis y Programación ☐ Consultores ☐ Sólo para ver

III. Acuerdo

Al firmar este documento, reconozco que soy responsable por la cuenta creada en el sistema a mi nombre. Además, certifico que he leído y me comprometo a cumplir con las normas y procedimientos establecidos en el "Manual de Normas sobre el Uso de Tecnologías de la Información". Entiendo que cualquier mal uso de la cuenta y accesos autorizados podría conllevar medidas disciplinarias establecidas en la reglamentación vigente del

_____ _____
Firma del(de la) Empleado(a) Fecha

IV. Política de Confidencialidad

Toda la información contenida en el sistema es confidencial, privilegiada y privada bajo la ley aplicable. La información se utilizará solamente para brindar servicios a los individuos o participantes del Departamento. Se prohíbe estrictamente la divulgación de información contenida en los sistemas a los cuales se le proveerá acceso.

_____ _____
Firma del(de la) Empleado(a) Fecha

V. Autorización del Supervisor

Certifico que este(a) empleado(a) requiere de las aplicaciones especiales antes solicitadas para llevar a cabo sus labores, por lo que esta solicitud cuenta con mi autorización.

_____ Nombre y Firma del(de la) Supervisor(a)

_____ Fecha

▼PARA SER COMPLETADO POR LA OFICINA DE SISTEMAS DE INFORMACIÓN▼

VI. Acción Tomada

Certifico que se evalúo la solicitud del(de la) empleado(a) y se tomó la siguiente determinación:

☐ Se dio(eron) el(los) acceso(s) solicitado(s).

☐ Se dio(eron) el(los) acceso(s) solicitado(s), excepto: _____

Razón: _____

☐ Se asignó contraseña provisional para acceder.

Nombre de(de la) Usuario(a): _____

Contraseña Asignada[1]: _____

Comentarios: _____

_____ Nombre y Firma del(de la) Representante Autorizado(a)

_____ Fecha

[1]El sistema formazará al usuario a cambiar esta contraseña la privera vez que la utilice.

DESCRIPCIÓN

El formulario DEFAM-520, "Solicitud de Acceso a Aplicaciones Especiales – ADSEF", lo utiliza el personal de la Administración de Desarrollo Socioeconómico de la Familia (ADSEF) para solicitar al personal de la Oficina de Sistemas de Información acceso a aplicaciones especiales.

INSTRUCCIONES GENERALES

Lea las siguientes instrucciones y complete cada una de las partes del formulario. Si algún encasillado no aplica, favor de escribir N/A.

I. Información del(de la) Usuario – Anote el nombre del(de la) usuario, clasificación, número telefónico de la oficina, correo electrónico, ubicación, oficina en que labora y cuenta de usuario.

II. Aplicaciones Especiales

   A. **Sistemas** – Seleccione la acción y el(los) acceso(s) que solicita.

   B. **Sistema de Administración e Información de Casos (SAIC y EBT)** – Indique la acción, puesto funcional y grupo asignado. Si no aplica, seleccione la alternativa provista para tal propósito en cada aplicación.

III. Acuerdo – Lea el acuerdo que conlleva la aprobación de aplicaciones especiales y certifique con su firma, y anote la fecha en que llevó a cabo tal acción.

IV. Política de Confidencialidad – Lea la política y certifique tal acciones estampando su firma y fecha en el espacio provisto.

V. Autorización del(de la) Supervisor(a) – En esta parte, el(la) supervisor(a) del(de la) empleado(a) certifica que los accesos a las aplicaciones especiales son necesarios. El(La) supervisor(a) anota su nombre, firma y escribe la fecha en que completó el documento.

VI. Acción Tomada – El(La) representante autorizado(a) certifica que evaluó la solicitud e indica la acción tomada. Además, asigna una contraseña provisional al usuario con la que podrá acceder las aplicaciones especiales; y anota la fecha en que completó el documento.

La Oficina de Sistemas de Información informará mediante correo electrónico la acción tomada (a la) director(a) de la oficina solicitante y al(a la) supervisor(a) del(de la) empleado(a) solicitante.

La política pública del Departamento de la Familia prohíbe el discrimen de clase alguna, entre otros motivos, por género. Por lo tanto, para propósitos de este documento, todo término que se utilice al mencionar una persona o puesto se refiere a ambos géneros.

Toda solicitud de corrección, revisión o derogación de este formulario debe ser tramitada a la Oficina de Sistemas y Procedimientos.

Mayo 2014

APÉNDICE 13

EMPLEADO DESIGNADO A COMPLETAR EL FORMULARIO DEFAM-82, CERTIFICACIÓN NEGATIVA DE ACCIONES DE PERSONAL

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

15 de julio de 2016

Nilda Muñoz Acosta, JD, MPA
Secretaria Auxiliar
Recursos Humanos y Relaciones Laborales

Blanca Pérez Torres
Directora
Oficina Sistemas de Información
Secretariado

RECURSOS DESIGNADOS PARA CERTICIFACION DEFAM-82

Conforme solicitado recientemente, sometemos para su conocimiento los nombres de los empleados de la Oficina de Sistemas de Información designados para certificar el documento Defam-82. El responsable primario de esta tarea será el Sr. Jesús Cruz, Supervisor de Sistemas II. En caso de que el Sr. Cruz por alguna razón no esté disponible, el Sr. José Flores – Supervisor de Procesamiento de Datos será la persona alterna designada.

Nos reiteramos a su disposición para clarificar cualquier duda que pueda surgir.

C. Jesús Cruz Supervisor Sistemas II
José Flores Supervisor Procesamiento de Datos

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

INSTRUCCIONES PARA PROCESAMIENTO FORMA
DEFAM-82 CERTIFICACION NEGATIVA DE ACCIONES DE PERSONAL

1. Las personas designadas para la firma de la forma DEFAM-82 son:

Jesús Cruz	Supervisor Sistemas II
José Flores	Supervisor Procesamiento de Datos

2. La persona designada verificará con el empleado solicitante de la Certificación si tenía equipo tecnológico asignado para ejercer sus funciones. En caso afirmativo, la persona designada firmará la Defam-82 **luego** de que Servicios Generales certifique que el empleado entregó la propiedad asignada. Si no tenía equipo tecnológico asignado puede firmarse la Defam sin que medie la firma de Servicios Generales.

3. La persona designada verificará con el empleado solicitante de la Certificación si tenía extensión telefónica asignada. De ser afirmativo, debe documentar el número de extensión en alguna parte de la Defam-82 y enviará correo electrónico al Sr. Howard Hatchett solicitando que declare vacante dicha extensión en el directorio electrónico.

4. La persona designada sacará copia de la DEFAM firmada y se la entregará a la secretaria para que la misma sea tramitada a la Sra. Jocelyn González, Oficinista de Entrada de Datos, solicitando que se proceda a dar de baja al empleado de los sistemas y aplicaciones a los que tenga acceso.

5. Jocelyn procesará la petición e informará mediante correo electrónico, la acción tomada a quien le haya tramitado la petición.

6. Es responsabilidad de las personas designadas el asegurarse que se procesen las peticiones de baja de los sistemas y la declaración de vacante de la extensión asignada al empleado.

Blanca Pérez Torres
Directora
Oficina Sistemas de Información
Secretariado

APÉNDICE 14

EJEMPLO DE ALERTA EMITIDO

Blanca I. Perez Torres

From: ServiceDesk <HelpDesk@netxar.com>
Sent: Wednesday, August 17, 2016 4:19 PM
To: FamiliaWAN
Subject: Incident 12422 Update Status

Incident 12422 Update Status Notification

Estatus con PRT:

Utuado
SF 138-8564 Ticket: 2016081600015
prob fibra/esc a sup de area

Summary
Familia-SF-138-8564-UtuadoI-RT has stopped responding (Request Timed Out)

Affected End User	Incident Area	Status	Priority
Hernandez, Miguel	Networks	Work In Progress	4

Reported By	Assignee	Group
Valentin, Maria	Valentin, Maria	

Severity	Urgency	Impact
		None

Incident Description
TIME OF EVENT MESSAGE 8/15/2016 10:48 AM Familia-SF-138-8564-UtuadoI-RT has stopped responding (Request Timed Out) 8/15/2016 10:47 AM Node Familia-SF-138-8564-UtuadoI-RT's packet loss has risen above 40% to 60 %.

APÉNDICE 15

AVISO INICIAL EN LA PANTALLA

Información Importante para los Empleados(as)

Advertencia sobre el uso del Sistema de Información Computadorizado

---

1. El sistema incluyendo los programas y los archivos electrónicos son propiedad del Secretariado y solo se utilizarán única y exclusivamente para fines estrictamente oficiales.
2. Ningún usuario deberá tener expectativas de intimidad con respecto a la comunicación electrónica de datos o información conservada o procesada a través de los sistemas del Secretariado.
3. No se deberá compartir o revelar la contraseña (password) propia o de ninguna otra persona. No Cambiar Wallpaper, no fotos personales, no musica de ambito personal o traer programas de sus hogares para ser instalados en los sistemas del Secretariado.
4. ENTIENDO y ACEPTO que cualquier violación a estas normas es causa suficiente para el inicio del proceso disciplinario que corresponda.
5. En definitiva, TODO EMPLEADO del Secretariado, está advertido del uso adecuado del equipo electrónico de la agencia.

Si usted desea más información, favor de solicitar copia de las directrices emitidas sobre la utilización de los sistemas a la Oficina de Informática.

OK

APÉNDICE 16

MANUAL DE NORMAS SOBRE EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN

Estado Libre Asociado de Puerto Rico
DEPARTAMENTO DE LA FAMILIA
Secretaría Auxiliar de Planificación e Informática
Oficina de Sistemas de Información

MANUAL DE NORMAS SOBRE EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN

Junio 2015

Estado Libre Asociado de Puerto Rico
Departamento de la Familia
Secretaría Auxiliar de Planificación e Informática
Oficina de Sistemas de Información

MANUAL SOBRE EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN

TABLA DE CONTENIDO

I. Introducción 1

II. Base Legal 1

III. Propósito 2

IV. Aplicabilidad 2

V. Definiciones 2

VI. Normas Aplicables a la Adquisición, Registro, Asignación, Uso y Conservación de los Sistemas de Información y a la Contratación de Servicios Profesionales 6

- A. Sistemas de Información 6
- B. Contratación de Servicios Profesionales 10

VII. Normas Aplicables a la Instalación de Programas, Confidencialidad y Seguridad de la Información 11

- A. Instalación de Programas 11
- B. Confidencialidad y Seguridad de Información 12
- C. Acceso Seguro a la Red Inalámbrica y Remota 15

VIII. Normas para Detectar, Reportar y Responder ante Incidentes de Seguridad 16

IX. Normas sobre Medidas Preventivas para Evitar Incidentes Mayores de los Sistemas de Información 18

X. Normas Aplicables para Controlar Accesos Físicos 19

XI. Normas para el Resguardo y Restablecimiento de Archivos 20

XII. Normas Aplicables al Uso del Correo Electrónico 21

XIII. Normas Aplicables al Uso, Manejo y Acceso del Internet 23

XIV. Normas de Uso de Redes Sociales 26

XV. Orientaciones 28

XVI. Oficial de Enlace 28

XVII. Acción Disciplinaria 28

XVIII. Cláusula de Salvedad 29

XIX. Cláusula de Separabilidad 29

XX. Enmienda 29

XXI. Derogación 29

XXII. Aprobación y Vigencia 29

Apéndices:

Apéndice 1 – DEFAM-482, "Designación de Representante Autorizado"

Apéndice 2 – DEFAM-311, "Transferencia Interna de Equipo"

I. INTRODUCCIÓN

En cumplimiento con la Ley Núm. 151 del 22 de junio de 2004, conocida como "Ley de Gobierno Electrónico", el Departamento de la Familia tiene la responsabilidad de garantizar el uso correcto de las tecnologías de información por parte de todos sus empleados(as) y funcionarios(as).

El Departamento de la Familia reconoce la importancia de establecer normas sobre el uso adecuado de sus sistemas electrónicos de información. Este Manual se considera una herramienta de referencia para los usuarios de sistemas de información sobre las políticas, estándares, prácticas de control y responsabilidad para el uso apropiado de la información, equipos, programas de aplicaciones en sus sistemas electrónicos de información.

II. BASE LEGAL

A. Plan de Reorganización Núm. 1 del Departamento de la Familia, según enmendado, aprobado el 28 de julio de 1995.

B. Ley Núm. 151 del 22 de junio de 2004, conocida como "Ley de Gobierno Electrónico".

C. Carta Circular Núm. 77-05 de 8 de diciembre de 2004 de la Oficina de Gerencia y Presupuesto; Política Núm. TIG-008.

D. Ley de Copyright, Copyright Act, 17 USCS § 106 y la Ley de Derechos de Autor.

E. Ley Núm. 96 del 15 de julio de 1988, según enmendada, conocida como "Ley de Propiedad Intelectual de Puerto Rico".

F. Procedimiento para el Recibo y Manejo de Activos Fijos aprobado el 19 de junio de 2003.

G. Reglamento Núm. 11, "Normas Básicas para el Control y la Contabilidad de los Activos Fijos", aprobado el 29 de diciembre de 2005.

III. PROPÓSITO

Este Manual tiene el propósito de establecer las normas relacionadas al uso de tecnologías de información en todos los componentes del Departamento de la Familia.

IV. APLICABILIDAD

Este Manual aplica a todos(as) los(as) empleados(as) y funcionarios(as) del Departamento de la Familia, y sus componentes programáticos y operacionales. De igual forma, aplica a cualquier consultor(a), contratista, sub-contratista o agencia delegada del Departamento o de alguna de sus Componentes, que por la naturaleza de su contrato o de su relación necesite utilizar las herramientas que se describen en este Manual.

La Ley Orgánica de la Administración para el Sustento de Menores en el Capítulo 25, Sección 506, Inciso O, faculta al Administrador "a determinar mediante Reglamento, aquellas reglas y normas necesarias para la conducción de los procesos administrativos...". De esta Administración no contar con un documento que indique los procesos establecidos en este Manual, puede adoptar el mismo.

V. DEFINICIONES

A. **Acción Disciplinaria** - Sanción recomendada por el(la) supervisor(a) del(de la) empleado(a) e impuesta por la autoridad nominadora, la cual pasa a formar parte del expediente del(de la) empleado(a). Ésta puede consistir de reprimendas escritas, suspensión de empleo y sueldo o destitución.

B. **Aplicación (*Software*)** - Sistema compuesto por programación y base de datos diseñados para automatizar funciones específicas de la Agencia. Existen dos (2) tipos de aplicaciones: aplicaciones comerciales o aplicaciones personalizadas.

C. **Archivo (*File*)** - Conjunto de datos almacenados en cualquier medio electrónico, tales como: computadoras, *usb flash drive, zip drive*, discos portátiles, servidores, etc. Un archivo tiene una identificación única formada por un "nombre" y un "apellido", en el que el nombre suele ser de libre elección del usuario y el apellido suele identificar el contenido o el tipo de archivo.

D. **Base de Datos (*Database*)** - Es el almacenamiento e integración colectiva de datos e información que son requeridas por organizaciones para cubrir sus requisitos de procesamiento.

E. **Centro de Cómputos** - Área de trabajo centralizada para el manejo de datos y comunicaciones, adscrita a la Oficina de Sistemas de Información.

F. **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.

G. **Clave de Acceso (*Password*)** - Código que utiliza el(la) usuario(a) para registrarse en la computadora y lograr acceso a la red u otras aplicaciones o bases de datos. La clave es cualquier conjunto de caracteres en el sistema computadorizado que identifique a un(a) usuario(a).

H. **Copiar** - Duplicar documentos, archivos, aplicaciones o programas.

I. **Correo Electrónico (*E-mail*)** - Sistema de correspondencia mediante transferencia electrónica que permite a los(as) usuarios(as) enviar o recibir mensajes, correos, archivos y almacenar los datos de los mensajes.

J. **Departamento** - Se refiere al Departamento de la Familia y sus componentes programáticos y operacionales, tales como: Secretariado, Administración para el Cuidado y Desarrollo Integral de la Niñez (ACUDEN), Administración de Desarrollo Socioeconómico de la Familia (ADSEF), Administración de Familias y Niños (ADFAN) y la Administración para el Sustento de Menores (ASUME).

K. **Director(a) de Sistemas de Información** - Persona responsable de planificar, organizar, coordinar, dirigir y supervisar todas las operaciones técnicas y administrativas generadas por las unidades de trabajo que integran la Oficina de Sistemas de Información.

L. **Encargado(a) de la Propiedad** - Empleado(a) designado(a) por el(la) Secretario(a) del Departamento o su Representante Autorizado y nombrado(a) por el(la) Secretario(a) de Hacienda como responsable del control y custodia de los activos fijos pertenecientes al Departamento.

M. **Enlace en Informática** - Título funcional de la persona encargada de administrar una red local, ofrecer apoyo tecnológico a los(as) usuarios(as) de una red, administrar contratos de servicios relacionados con la tecnología y coordinar los asuntos relacionados a sistemas de información de un componente del Departamento (ACUDEN, ADFAN y ADSEF. Aplicará a la ASUME si su estructura así lo establece.).

N. **Estación de Trabajo** - Con su sistema operativo asociado, provee la interfaz entre el(la) usuario(a) a las aplicaciones existentes. Pueden incluir: computadoras personales (PC), terminales controlados por sistemas centrales (*thin client*), interfaces de voz, dispositivos móviles de una o múltiples funciones (*Pocket PC*, PDA, teléfonos PDA, etc.), dispositivos telefónicos, entre otros.

O. **Licencias** - Es un contrato entre el(la) autor(a) del programa y el(la) usuario(a), que le permite al(a la) adquiriente de la licencia utilizar el programa de forma legal.

P. **Oficina de Sistemas de Información (OSI)** - Oficina adscrita a la Secretaría Auxiliar de Planificación donde se planifican, organizan, apoyan, dirigen y supervisan las operaciones tecnológicas diarias y comunes a los componentes del Departamento; entiéndase equipos, sistemas de telecomunicaciones, correo electrónico, internet, aplicaciones, entre otros.

Q. **Periferales (Equipo Periférico)** - Aparatos o equipos electrónicos, tales como: impresoras, *scanners*, *mouse*, teclado, proyector, *drives*, y otros equipos conectados externamente a un puerto de la computadora.

R. **Programa** - Conjunto de instrucciones que permite que una computadora lleve a cabo una función. Puede haber programas de sistema 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.

S. **Red *(Network)*** - Sistema de telecomunicación para transferencia de datos que conectan entre sí a los sistemas de información. Conjunto de equipos y programas electrónicos interconectadas por varios tipos de dispositivos de telecomunicaciones.

T. **Red de Área Amplia (*Wide Area Network (WAN)*)** - Red de computadoras personales conectadas entre sí por sistemas de telecomunicaciones en áreas geográficas extensas.

U. **Red inalámbrica** (*Wireless Network*) - Red que se comunica por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

V. **Red Local (*Local Area Network (LAN)*)** - Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajos, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones y los recursos disponibles en la red.

W. **Representante Autorizado** - Persona designada por un nivel jerárquico superior para efectuar una tarea a nombre de la persona que lo designa. La designación del representante autorizado se hace mediante el uso del formulario DEFAM-482, "Designación de Representante Autorizado". Apéndice 1.

X. **Resguardo (*Backup*)** - Se define como la actividad de copiar archivos, datos o datos magnéticos contenidos en un medio de almacenamiento de origen a un medio de almacenamiento alterno de forma que estén disponibles en caso de que un fallo produzca la pérdida de los archivos.

Y. **Secretaria(o) Auxiliar de Planificación e Informática** - Persona designada por la Secretaria(o) para planificar , coordinar, dirigir, supervisar y evaluar todas las actividades que se desarrollan en las oficinas adscritas a la Secretaría Auxiliar de Planificación e Informática, entre estas, la Oficina de Sistemas de Información. Participa activamente en la formulación de la política pública de su área de trabajo y en la dirección y supervisión de los proyectos estratégicos de tecnología del Departamento de la Familia.

Z. **Servidor (*Server*)** - Es una computadora con su respectivo sistema operativo capaz de proveer servicio a múltiples estaciones de trabajo. Entre los servicios disponibles se encuentran el manejo de archivo, impresión o comunicaciones.

AA. **Sistemas** - Conjunto de programación, equipos de telecomunicaciones, servidores y periféricos que se utilizan para la recopilación, almacenamiento, análisis, gerencia, control e intercambio de datos.

BB. **Tecnologías de la Información (*Information Technology*)** - Ciencia relacionada con el procesamiento de datos y procesos automáticos para el manejo de información.

CC. **Telecomunicaciones** - Toda transmisión de señales, imágenes, sonidos, voz o datos mediante sistemas electrónicos.

DD. **Usuario(a)** - Todo(a) empleado(a), contratista independiente, sub-contratista y cualquier otra persona o entidad que esté autorizado(a) a tener acceso o utilice los recursos y servicios de tecnología del Departamento.

EE. **Virus** - Programa cuyo fin es hacer algún tipo de daño a la computadora donde se aloja.

VI. NORMAS APLICABLES A LA ADQUISICIÓN, REGISTRO, ASIGNACIÓN, USO Y CONSERVACIÓN DE LOS SISTEMAS DE INFORMACIÓN Y A LA CONTRATACIÓN DE SERVICIOS PROFESIONALES

A. Sistemas de Información

1. Adquisición

a. El Enlace en Informática de cada componente solicitará la aprobación por escrito al(a la) Director(a) de la Oficina de Sistemas de Información (OSI), previo a la compra de cualquier equipo tecnológico, programas y licencias. La solicitud debe estar acompañada por un documento donde se justifique la compra, indique la procedencia de los fondos y el alcance para los cuales los dispositivos se utilizarán.

b. Luego de recibir la aprobación, el Enlace en Informática de cada componente gestiona la adquisición siguiendo el procedimiento establecido. La compra se lleva a cabo según establecido en la reglamentación vigente.

c. El(La) Director(a) de la OSI, o su representante autorizado, y los Enlaces en Informática tienen que asegurar que todas las computadoras personales se adquieran con su respectivo conjunto de *software* y que tengan sus certificados de autenticidad.

2. **Registro**

a. Todo equipo tecnológico, programas y licencias adquiridas por el Departamento se registran en la OSI y en el caso de las Administraciones, el Enlace en Informática lleva el registro. Esta información será remitida semestralmente a la OSI que será responsable a su vez de mantener un registro actualizado a nivel de la Agencia. Esto no sustituye los procedimientos establecidos por la División de Propiedad del Departamento, las disposiciones de reglamentación vigente del Departamento de Hacienda, ni las responsabilidades del(de la) Encargado(a) de la Propiedad. Este registro debe contener el número de propiedad asignado, el número de serie del equipo, la fecha de adquisición y el nombre del(de la) usuario(a) a quien se le asignó el equipo.

b. Todo programa o licencia de autenticidad la debe custodiar la OSI o el Enlace en Informática de cada componente, según sea el caso, una vez el(la) encargado(a) de la propiedad le asigne número. El personal de sistemas de información instala los programas y lleva un registro, para así cumplir con los requisitos de licenciamiento. Anualmente, el Enlace en Informática somete copia del registro de licencias a la OSI.

3. **Asignación**

a. El(La) Secretario(a), los(as) Administradores(as) o sus representantes autorizados asignan las computadoras personales o portátiles a aquellos(as) empleados(as) o funcionarios(as) que necesitan esta herramienta para desempeñar las funciones de su puesto.

b. El(la) Secretario(a), los(as) Administradores(as) o sus representantes autorizados determinan las necesidades de equipo de cada usuario y se reservan el derecho de intercambiar las computadoras y sus periferales, según las necesidades del Departamento.

c. Las computadoras personales y portátiles asignadas a los(as) usuarios(as) son propiedad del Departamento y están destinadas para uso oficial dentro de las funciones de éstos en el Departamento.

4. **Transferencia**

a. El(La) Secretario(a), Administrador(a) o su representante autorizado puede autorizar la transferencia de equipo, programas o licencias tecnológicas, siempre que se cumpla con la reglamentación vigente de la División de Propiedad y el Departamento de Hacienda.

b. Los(as) Directores(as) Regionales y Locales preparan un informe escrito de las transferencias realizadas y lo presentan al Enlace en Informática de la Administración correspondiente en junio y diciembre de cada año.

c. El(La) Encargado(a) de la Propiedad que reciba una transferencia o una solicitud para dar de baja este tipo de equipo, debe asegurarse de que exista una autorización por escrito y debe informar a la OSI o al(a la) Oficial en Informática, según aplique, el resultado del proceso realizado.

d. En toda transacción de préstamo de equipo entre empleados(as) debe mediar una Transferencia Interna de Equipo, DEFAM-311, según establecido en el "Procedimiento para el Recibo y Manejo de los Activos Fijos". Apéndice 2

5. **Uso y Conservación**

a. El(La) usuario(a) a quien se le asigne una computadora es el(la) principal responsable del uso y conservación de ésta, y del equipo periférico que se añada. Este equipo puede constar de computadora personal o portátil y equipo periférico, como: impresora, teclado, *mouse, pen drives*, proyector, *scanner*, entre otros.

b. La OSI o el Enlace en Informática colocará un aviso que indique al(a la) usuario(a) o a quien acceda a su sistema de información que está accediendo a un sistema de información propiedad del Departamento de la Familia del Estado Libre Asociado de Puerto Rico y que se compromete a utilizarlo conforme a las normas establecidas.

c. A cada usuario(a) se le entrega la computadora configurada y autorizada con aquellos programas necesarios para cumplir con las funciones que le correspondan.

d. Aquellos(as) usuarios(as) a los(as) que se le asignen computadoras portátiles son responsables de cuidar la unidad y protegerla de daño físico. Además, deben ser resguardadas para evitar la exposición al calor, exposición directa al sol y la humedad por tiempo prolongado, ya que el equipo puede sufrir daños. Se excluye de esta norma los daños ocasionados por el deterioro normal del equipo por su uso a través del tiempo, daños por accidente y hurtos en que no medie culpa, falta o negligencia por parte del (de la) usuario(a).

e. Para evitar hurtos, las computadoras portátiles no pueden ser dejadas en los vehículos debido a la proliferación de técnicas o sistemas utilizados para identificar la existencia de estas en los vehículos aun cuando estén ocultas.

f. Los sistemas deben activar automáticamente el protector de pantalla establecido para bloquear el acceso a esa computadora una vez transcurran 15 minutos sin que se detecte actividad en la computadora. Una vez se active, la persona tiene que volver a registrar su cuenta de usuario y clave para acceder.

g. El(La) usuario(a) tiene que registrar una contraseña para reactivar la computadora.

h. El(La) usuario(a) es responsable de bloquear su cuenta de acceso a la computadora cada vez que se aleje de su estación de trabajo.

i. Para asegurar la integridad del equipo y evitar que la red de información se afecte por la transmisión y presencia de algún virus, al(a la) usuario(a) se le prohíbe lo siguiente:

1) Hacer cambios a la configuración de la computadora asignada.
2) Conectar a una computadora un equipo periférico que no haya sido aprobado o adquirido por el Departamento, sin previa autorización de la OSI, representante autorizado(a) o del Enlace en Informática del componente.
3) Reparar por sí mismo el equipo cuando ocurra una avería. Si el equipo requiere reparación, el(la) usuario(a) debe comunicarlo de inmediato a la OSI o al(a la) Enlace en Informática.
4) Ingerir alimentos o bebidas cerca del área de la computadora para así evitar accidentes y daños al equipo.
5) Mutilar el equipo computarizado por medio de marcas y escritos. No colocar pegatinas ni magnetos en el equipo asignado, excepto los provistos por la División de Propiedad para propósitos de inventario.
6) Dejar el equipo en su automóvil o llevárselo para su casa sin estar debidamente autorizado, ya que estaría expuesto a apropiación ilegal, robo u otra causalidad, como por ejemplo, daños por accidentes.

6. **Auditorías**

a. El Departamento está sujeto a auditorías periódicas para examinar los sistemas computarizados por parte de la Oficina del Contralor de Puerto Rico, Oficina de Gerencia y Presupuesto, Oficina de Auditoría Interna, entre otras.

B. Contratación de Servicios Profesionales

1. La OSI debe asegurarse de que las cláusulas de los contratos de servicios profesionales y consultivos estén acorde con las cartas circulares que emite la Oficina de Gerencia y Presupuesto, y las leyes vigentes que apliquen. La

2. contratación podrá incluir cláusulas de transferencia de conocimientos en aquellos casos que sea pertinente.
3. Los sistemas desarrollados por los componentes del Departamento deben incluir las disposiciones reglamentarias para los derechos del(de la) autor(a), la entrega del código fuente, documentación adecuada y niveles de servicios óptimos para el Departamento.
4. Los contratos de servicios profesionales de tecnologías deben contar con la aprobación del(de la) Director(a) de la OSI, previo a la firma del(de la) Secretario(a). Estos contratos deben estar acompañados por una comunicación donde se justifique la contratación de estos servicios, la procedencia de los fondos y el borrador del contrato a otorgarse.

VII. NORMAS APLICABLES A LA INSTALACIÓN DE PROGRAMAS, CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

A. Instalación de Programas

1. Ningún(a) usuario(a) está autorizado(a) a instalar programas en las computadoras o eliminar programas previamente instalados, sin el debido consentimiento de la OSI o del Enlace en Informática de su componente.
2. El(La) usuario(a) no está autorizado(a) a realizar cambios de configuración en su estación de trabajo o en cualquier computadora, servidor, o sistema "Mainframe" en el Departamento. Esto incluye añadir, modificar o eliminar dispositivos periféricos, sonido, o apariencia de pantalla (*wallpaper* y/o *screen saver)*, entre otros.
3. Se prohíbe copiar programas protegidos por las leyes de derecho de autor(a) o instalar programas sin licencias. Los equipos asignados a los(as) empleados(as) y funcionarios(as) tienen instalados programas cuyas licencias han sido adquiridas por el Departamento. Cualquier necesidad de programas o licencias, se canaliza a través de la OSI o del Enlace en Informática de su componente. El Departamento no requiere, solicita, ni condona la duplicación o uso no autorizado de programas protegidos por derecho de autor(a).

4. El personal de sistemas de información son los únicos autorizados a instalar y configurar *software* comprado en todos los sistemas de computadora del Departamento. Además, son responsables de remover cualquier *software* instalado sin autorización por los usuarios.
5. Para solicitar acceso a los sistemas, el(la) usuario(a) debe completar el formulario DEFAM-516, Solicitud de Acceso a los Sistemas; y para solicitar acceso a la internet, el DEFAM-517, Solicitud de Acceso al Internet. En cuanto al acceso a aplicaciones especiales, el(la) usuario(a) debe completar el formulario "Solicitud de Acceso a Aplicaciones Especiales", que corresponde al componente en donde trabaja.

B. **Confidencialidad y Seguridad de la Información**

1. La información manejada por las aplicaciones del Departamento de la Familia es propiedad del Estado Libre Asociado de Puerto Rico, y como tal, la gerencia del Departamento se reserva el derecho y los privilegios de tener acceso a la misma.
2. Toda la información y datos generales en los sistemas del Departamento son considerados activos del Departamento de la Familia y del Estado Libre Asociado de Puerto Rico, lo que significa que inmediatamente se convierte en información confidencial y tiene que protegerse de accesos o divulgación no autorizada.
3. Toda información relacionada al curso operacional del Departamento que se genera y conserva en la computadora debe mantenerse de forma confidencial de acuerdo a la legislación y reglamentación vigente, y aplicable a los Departamentos y entidades públicas del Estado Libre Asociado de Puerto Rico.
4. Los documentos generados o contenidos en los sistemas de información del Departamento serán parte de los expedientes oficiales. La destrucción de tales documentos electrónicos sin la debida autorización estará sujeta a las sanciones aplicables a la destrucción de documentos públicos.

5. Ninguna información debe sacarse fuera de las instalaciones o compartirse con externos u otro personal de diferentes niveles de acceso.
6. Toda información que genera el(la) usuario(a) se conservará en los discos duros de los servidores. Todos los días los(as) empleados(as) encargados(as) de estos servidores llevarán a cabo procesos de resguardo (*backup*) con el propósito de almacenar esta información en el sistema adoptado para hacer resguardos. Los datos resguardados en el medio seleccionado serán almacenados en facilidades externas que sean adecuadas y serán usados para restaurar la información en caso de ser necesario.
7. Todo(a) usuario(a) de computadora portátil (*laptop*) que no esté conectado(a) a la red será responsable de efectuar un proceso de resguardo (*backup*) en un medio físico externo de su selección (CD, DVD o *pen drive*).
8. La OSI o el Enlace en Informática de cada componente, según aplique, provee las claves de acceso temporero a las unidades asignadas, posteriormente los(as) usuarios(as) cambian la clave para asegurar que otra persona no pueda acceder a su sistema. Cada usuario(a) será responsable por el manejo adecuado de su código de acceso o contraseña asignada. La clave de acceso otorgada incluye el servicio de correo electrónico.
9. La clave de accesos será regida por los siguientes parámetros de seguridad: la contraseña del(de la) usuario(a) deberá ser de un mínimo de ocho (8) caracteres y contener una combinación de números y letras. La contraseña deberá ser cambiada en un plazo menor a 180 días y no podrá repetir las últimas cinco (5) contraseñas utilizadas en el sistema. Si el(la) usuario(a) falla tres intentos con la clave de su cuenta, el sistema bloqueará la cuenta y el(la) usuario(a) debe solicitar apoyo técnico al personal de sistemas de información correspondiente.
10. Las cuentas no utilizadas por un término de 45 días serán inactivadas automáticamente por el sistema.

11. Todo(a) empleado(a) que cese funciones, ya sea por renuncia o traslado a otro componente debe solicitar a la OSI o al Enlace en Informática, según sea el caso, que le complete el apartado correspondiente en el formulario DEFAM-82, Certificación Negativa de Acciones de Personal.
12. Los(as) usuarios(as) no deben dejar su clave de acceso a los sistemas de información grabada o escrita en la computadora, escritorio u otro lugar accesible a otros(as) empleados(as) o terceras personas. Las claves de acceso asignadas deben ser protegidas por los(las) usuarios(as) y no deben ser compartidas ni divulgadas. El(La) usuario(a) autorizado(a) es responsable por todo cuanto suceda o acontezca a través de su cuenta como consecuencia de su utilización o por descuido de este(a) y toda acción que esté bajo su control.
13. Todo personal que tenga acceso a datos de computadora, que haya sido despedido o transferido entre Oficinas, se le debe revocar los privilegios de acceso a datos de computadora el mismo día del despedido, transferencia o promoción.
14. La Oficina de Recursos Humanos tiene que notificar de inmediato a la OSI o al Enlace de Informática, según sea el caso, cuando un(a) empleado(a) se haya despedido o transferido a otra área de trabajo para la inactivación inmediata de sus accesos.
15. Si el(la) usuario(a) tiene que retirarse de su escritorio debe cerrar todas las aplicaciones que se encuentren abiertas en su computadora. Además, debe apagar la computadora en caso de abandonar el área de trabajo por tiempo prolongado, o cuando no regrese a su lugar de trabajo, para evitar dejar documentos u hojas de trabajo abiertas y accesibles.
16. La divulgación de información sin autorización está estrictamente prohibida. La alteración fraudulenta de cualquier documento en formato electrónico conllevará las sanciones aplicables a la alteración fraudulenta de documentos públicos.
17. La OSI y el Enlace en Informática de cada componente son los responsables de mantener la seguridad dentro de la red contra los ataques externos en forma de

virus, *malware*, *phising*, etc. Para esto utilizan las herramientas provistas por la Oficina de Gerencia y Presupuesto (OGP).

18. La OSI y el Enlace en Informática de cada componente tienen que proteger el acceso no autorizado a la información utilizando métodos fiables de detección de intrusos. Los métodos disponibles pueden incluir el encriptado, firmas digitales, autoridades de certificados, servidor de seguridad, *software* de acceso lógico y otros métodos.
19. Antes de utilizar CD/DVD, *pen drives* o discos duros externos en los equipos de la agencia, el usuario debe revisarlos a través de un programa antivirus, ya que los mismos pueden contener archivos infectados que pueden introducirse en la red de computadoras y contaminarla.
20. No se pueden colocar artefactos electrónicos, radios, amplificadores o toca disco compacto, que utilicen imanes internamente, cerca de ningún equipo o medio de computadora.
21. Los(as) consultores(as) externos(as), personas contratadas o subcontratistas se harán responsables si durante la ejecución de sus tareas no protegen la integridad o confidencialidad de la información del Departamento.
22. Cualquier situación que pueda poner en peligro la seguridad o cualquier otro control relacionado a información se debe comunicar inmediatamente a la OSI o al Enlace en Informática del componente.
23. El acceso físico al Centro de Cómputos está restringido a personal autorizado con el propósito de prevenir la destrucción maliciosa o accidental de información, equipos de sistema, datos o facilidades, o acciones que puedan, de alguna manera, impedir el funcionamiento correcto y/o manejo de dicho equipo, datos o instalaciones.

C. **Acceso Seguro a la Red Inalámbrica y Remota**

1. El Departamento de la Familia delega en el/la Directora/a de la OSI la responsabilidad de suministrar redes inalámbricas (WLAN o LAWN, por sus

siglas en inglés) para permitir conectividad móvil y flexible a las redes locales y al *Internet*.

2. La OSI suministra acceso inalámbrico a una red que sea viable; donde la infraestructura esté disponible, y los requerimientos técnicos y de seguridad permitan su utilización.
3. La implantación de acceso inalámbrico se coordinará a través de la OSI y el Enlace en Informática de cada componente. Ésta es responsable de configurar el *WLAN* de modo que la conexión sea segura y que se garantice la integridad de las redes, sistemas, aplicaciones y datos mediante la implantación de técnicas de segmentación y autenticación.
4. El acceso a las redes del Departamento solo se otorgará a aquellas personas cuyas funciones de trabajo requieran dicho acceso.
5. Las personas que utilicen redes de datos públicos para llevar a cabo actividades del Departamento tienen que estar autorizadas por el(la) supervisor(a) a quien se reportan, para poder recibir el(los) número(s) de cuenta y las identificaciones de usuarios.
6. Es responsabilidad de la OSI y los Enlaces en Informática asegurar que la red del Departamento sigue las normas de seguridad establecidas por el Departamento para todos los usuarios de sistemas de información.
7. Los(as) usuarios(as) con necesidades de acceso remoto que no sean empleados(as), tales como clientes y contratistas, tienen que ser autorizados adecuadamente por el personal autorizado de la OSI o el Enlace en Informática del componente.

VIII. NORMAS PARA DETECTAR, REPORTAR Y RESPONDER ANTE INCIDENTES DE SEGURIDAD

A. La Oficina de Sistemas de Información (OSI) es responsable de informar a los usuarios sobre las actividades que constituyen violaciones a las normas establecidas sobre el buen uso de los sistemas de información.

B. La OSI tiene que asegurarse de que todos los sistemas que manejen información sensitiva, crítica y variable del Departamento generen registros para mostrar cada adición, modificación y eliminación de información.

C. La OSI es responsable de que los récords de registros de computadora se mantengan seguros y con copia de seguridad por seis(6) años, en caso de que se necesiten para una investigación o para cuando la gerencia quiera saber quién ha llevado a cabo ciertas acciones en un sistema o red. Además, deben establecer un control sobre el acceso a los registros, de manera que sea para uso exclusivo de personal autorizado.

D. Los(as) usuarios(as) son responsables de cualquier actividad registrada por el sistema en donde su cuenta de identificación de usuario se haya registrado. Estas actividades, así como cualquier cambio, se registran en el sistema automáticamente.

E. El(La) encargado(a) de la red o su representante autorizado debe monitorear las actividades del sistema y darle seguimiento a sospechas de intentos de violación de acceso. Aun los intentos inválidos de obtener acceso a cualquier sistema se registran.

F. Los(as) usuarios(as) son responsables de notificar de inmediato a su supervisor cualquier problema que confronten con el acceso a los sistemas. Los(as) supervisores(as), a su vez, notifican al encargado de la red o su representante autorizado para buscar una solución inmediata al problema.

G. Todo(a) usuario(a) del sistema es responsable de informar de inmediato, a su supervisor(a) inmediato(a), por escrito cualquier sospecha de incidente, problema o violación de seguridad.

H. Los(as) supervisores(as) inmediatos(as) tienen que informar de inmediato al(a la) encargado(a) de la red de su componente cualquier incidente, problema o violación de seguridad. Este(a) será responsable de investigar y validar la naturaleza del incidente, así como, fortalecer las características de seguridad para evitar que ocurra en el futuro.

I. La OSI debe establecer canales de comunicación anónima disponibles para que los(as) empleados(a) puedan notificar incidentes de violación sin necesidad de identificarse.

J. El(La) usuario(a) que sospeche que otra persona conoce el ID de su cuenta de acceso y contraseña tiene que notificar de inmediato esta situación al área de seguridad de la OSI, para librarse de responsabilidad y configurar una contraseña nueva.

IX. NORMAS SOBRE MEDIDAS PREVENTIVAS PARA EVITAR INCIDENTES MAYORES DE LOS SISTEMAS DE INFORMACIÓN

A. Como parte del uso diario de los sistemas de información, los(as) empleados(as) deben:

1. Cerrar los archivos cuando no estén en uso, de manera que la información no esté accesible.
2. Proteger toda la información sensitiva mientras la imprima en una impresora común o compartida, siempre y cuando esté al alcance.
3. Guardar su trabajo cada 10–15 minutos para evitar la pérdida de información en caso de un bajón o apagón de luz. Pueden solicitarle a la OSI o al Enlace en Informática que configuren este aspecto y la computadora automáticamente ejecute la función de resguardo.
4. Efectuar un resguardo de sus archivos de información diariamente. Recuerde que si está conectado y grabando los archivos en el disco de la Red, no es necesario que ejecute la función de respaldo, ya que la OSI tiene un sistema de resguardo de información general que guardará su información automáticamente. Este resguardo se ejecuta durante los procesos operacionales nocturnos de los sistemas de información.
5. De necesitar que la OSI ejecute un resguardo de su información fuera del horario establecido, deberá solicitar por escrito dicha gestión.

B. Como medida de protección del equipo contra robo y acceso no autorizado, el(la) encargado(a) interno(a) de la propiedad de cada oficina o persona designada debe:

1. Mantener un inventario al día de todo el equipo en su área de trabajo.
2. Mantener sus discos y programas en un lugar seguro fuera de su área de trabajo.
3. Inspeccionar a fondo el equipo prestado cuando se le devuelva y cumplir con los procedimientos o reglamentación relacionada a activos fijos establecida por la División de Propiedad.
4. No prestar ninguna pieza de equipo a personal que planifique utilizarlo fuera del DEPARTAMENTO DE LA FAMILIA o fuera de la oficina sin la autorización apropiada y registro adecuado.

C. Como medida de protección contra daño físico del equipo, los(as) empleados(as) deben:

1. Evitar movimientos del equipo.
2. Usar el protector contra irregularidades de voltaje (UPS) en su equipo en todo momento, por lo que no deben desconectarlo sin autorización de la OSI.
3. No colocar otro equipo electrónico (radios, televisión) en la misma toma eléctrica de su sistema de información.
4. No colocar comida ni bebidas cerca de su sistema de información.
5. No colocar ningún tipo de plantas o flores naturales sobre sus equipos computadorizados.
6. No colocar libretas ni ningún artículo sobre las áreas de ventilación de la computadora.
7. No utilizar grapas o presillas de metal cerca del teclado de la computadora.
8. No forzar un dispositivo de resguardo (*backup*) en los puertos de su computadora.
9. No fumar, comer o beber cerca de su computadora.

X. NORMAS APLICABLES PARA CONTROLAR ACCESOS FÍSICOS

A. La Oficina de Seguridad y Manejo de Emergencias, o como se le denomine en cada componente, es responsable de evitar el acceso físico no deseado a los sistemas de información por medio de las siguientes acciones, entre otras:

1. Controlar el acceso al edificio por medio de guardia de seguridad y registro de visitantes.
2. No identificar la ubicación del área de centro de cómputos en los directorios o tablones de edictos.
3. Mantener un control de acceso electrónico en la OSI y lugares donde se encuentran los servidores; y proveer al personal acceso de acuerdo a su área de trabajo. Aplica solo en los lugares en donde existan controles de acceso electrónico.

B. La OSI cuenta con los siguientes controles de acceso:

1. Acceso Área Común – Cada persona que no sea empleado(a) de la OSI que tenga que acceder para ejercer funciones oficiales, deberá firmar en el registro o bitácora de acceso. Toda visita firmará su ingreso al área.
2. Acceso al Área Restringida del Centro de Cómputos – Esta área tiene un panel de seguridad con clave asignada al personal autorizado de sistemas de información.
3. Personal No Autorizado – Queda terminantemente prohibido a todo personal que no esté en funciones oficiales permanecer en la Oficina de Sistemas de Información.

XI. NORMAS PARA EL RESGUARDO Y RESTABLECIMIENTO DE ARCHIVOS

A. La OSI y los Enlaces en Informática son responsables de crear copias de resguardo de los archivos de información, de manera que puedan ser utilizados cuando se pierda o accidentalmente se borre el disco duro.

B. La OSI y los Enlaces en Informática de cada componente serán responsables de crear directorios para guardar los archivos del sistema en el servidor designado para el resguardo de información de usuarios.

C. Los(as) usuarios(as) que deseen guardar sus archivos en directorios de acuerdo a su área de trabajo son responsables de guardar y establecer un sistema de almacenamiento que facilite el resguardo y recuperación de información.

D. Los(as) usuarios(as) deberán guardar sus documentos en el área asignada para almacenar documentos.

E. Se seguirán las normas y los procedimientos establecidos en la reglamentación vigente relacionada a resguardo de información.

XII. NORMAS APLICABLES AL USO DEL CORREO ELECTRÓNICO

A. Los(Las) usuarios(as) del correo electrónico están obligados(as) a respetar los derechos de otros(as) usuarios(as), respetar la integridad de los sistemas y recursos físicos relacionados, y observar las leyes, reglamentos y obligaciones contractuales relevantes.

B. Los sistemas de comunicación o correo electrónico y toda información contenida en los mismos son propiedad del Departamento; por lo que, toda la información y mensajes creados y enviados a través de los sistemas se consideran expedientes y documentos oficiales del Departamento.

C. El correo electrónico se utiliza únicamente para propósitos oficiales relativos a las funciones de la Agencia.

D. El correo electrónico es una herramienta de trabajo que se otorga con el propósito de agilizar los trabajos del Departamento.

E. Para el envío de documentos que contengan información sobre asuntos internos del Departamento que deban ser cifrados (*encrypted*) se debe solicitar asistencia al personal de la OSI o al Enlace en Informática. De sospecharse que la información fue interceptada o divulgada, debe informarse de inmediato a la OSI o al Enlace en Informática, de manera que se tomen las medidas cautelares que procedan, de acuerdo a la particularidad de cada caso.

F. El contenido y mantenimiento del buzón electrónico es responsabilidad de los(as) usuarios(as), por lo que deben:

1. Verificar el correo electrónico diariamente.
2. Eliminar inmediatamente los mensajes no deseados, ya que estos ocupan espacio en el disco.

3. Mantener a un mínimo los mensajes retenidos en su buzón.

G. Todo mensaje de correo electrónico llevará escrito en la parte inferior del documento una advertencia de **"Nota de Confidencialidad"** que protege los derechos de confidencialidad del Departamento, igual o similar a la siguiente:

"Aviso de confidencialidad:

Este correo electrónico, y cualquier documento adjunto, contiene información propietaria, confidencial y/o privilegiada, perteneciente al Departamento de Familia. Se advierte que cualquier divulgación, distribución, copia o acción relacionada al contenido de esta comunicación que sea realizada sin la autorización del remitente está prohibida por ley. De usted no ser el destinatario intencionado o de haber recibido este mensaje por error, se le solicita que proceda a su eliminación, así como a la de cualquier documento adjunto al mismo, y que de forma inmediata nos lo notifique mediante correo electrónico remitido a nuestra atención o llamando a nuestras oficinas al (787) 294-4900. El Departamento de la Familia ha tomado las precauciones necesarias para asegurar que el envío del presente correo electrónico se encuentre libre de virus y/o contenido malicioso. No obstante, no podemos asegurar que así sea, por lo cual no nos hacemos responsables de cualquier daño atribuible al caso."

"Confidentiality Note:

This e-mail, along with any other document attached herein, contains proprietary, confidential and/or privileged information belonging to the Puerto Rico Department of the Family. You are hereby warned that any dissemination, disclosure, distribution, reproduction or the taking of any action in reference to the contents of this communication, without the consent of the sender, is strictly forbidden by law. If you are not the intended recipient or have received the current message by mistake, you are required to proceed with its immediate destruction and/or elimination, and notify the sender at once through the shown e-mail address or call our offices at (787) 294-4900. The Department of the Family has taken all precautionary measures to ensure the remittance of e-mail communications are free of viruses and/or any other malicious content. However, we cannot guarantee that this is the case, for which we disclaim any responsibility over any damage attributable thereto."

H. La OSI será responsable de establecer controles en el tiempo (no más de 30 días) que se conservarán los correos electrónicos almacenados en los sistemas. Dicha Oficina se reserva el derecho de borrar los mensajes de correo electrónico, ya que será responsabilidad del usuario salvaguardar aquellos mensajes que desee conservar como documento de trabajo o de referencia.

I. El(La) usuario(a) del correo electrónico es responsable por el uso de su cuenta, por salvaguardar su contraseña y no divulgarla.

J. Se prohíbe que los(as) empleados(a) y funcionarios(as) utilicen sus cuentas personales de correo electrónico en los equipos del Departamento. Se exime del cumplimiento de esta regla, con el visto bueno de la OSI o el Enlace en Informática de cada componente, a algunos(as) empleados y funcionarios(as) que ocupen unos puestos que debido a la naturaleza de sus funciones necesitan acceder información mediante su cuenta personal.

K. Está prohibido utilizar el correo electrónico para enviar mensajes personales o que puedan considerarse irresponsables, molestosos, hostigantes u ofensivos, incluyendo todo comentario o imagen de contenido sexual, pornográfico, obsceno o racista y utilizar lenguaje descortés o soez, mensajes en cadena o chistes.

L. Está prohibido utilizar el correo electrónico para recibir o enviar programas protegidos por las leyes de derecho de autor(a).

M. La divulgación de información contenida en un correo electrónico sin autorización está estrictamente prohibida. La alteración fraudulenta de cualquier documento en formato electrónico conllevará las sanciones aplicables a la alteración fraudulenta de documentos públicos.

XIII. NORMAS APLICABLES AL USO, MANEJO Y ACCESO DEL INTERNET

A. Los sistemas de comunicación y el acceso al internet son propiedad del Departamento y sus componentes. Se brindará acceso a la internet a los(as) usuarios(as) que como parte esencial de sus funciones lo requieran como herramienta de trabajo.

B. El acceso a la internet es conferido única y exclusivamente por el(la) Secretario(a), Subsecretario(a), Ayudante Ejecutivo(a), Secretarios(as) Auxiliares y Administradores(as), o sus representantes autorizados; tomando en consideración la necesidad para los servicios, la disponibilidad de ancho de banda, y la seguridad de las redes y comunicaciones.

C. Todo empleado que necesite utilizar datos públicos, tales como: internet o intranet, para realizar sus tareas, debe solicitar el acceso y tener la autorización de su supervisor con su correspondiente justificación.

D. La OSI y los Enlaces en Informática llevarán un registro de los(as) empleados(as), funcionarios(as) y personas contratadas que tienen acceso a información por medio de redes de datos públicos, tales como el internet y el intranet.

E. La OSI y los Enlaces en Informática configurarán la creación de un registro para los sitios del *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.

F. Los(as) usuarios(as) del internet deben respetar los derechos de otros(as) usuarios(as), respetar la integridad de los sistemas y recursos físicos relacionados, y observar las leyes, reglamentos y obligaciones contractuales, respectivamente. Además, deben asegurarse de no poner en riesgo la seguridad, niveles de servicio ni la reputación del Departamento con el acceso a página de internet no autorizadas.

G. El(la) usuario(a) de internet es responsable por el uso de su cuenta y de salvaguardar su contraseña y no divulgarla.

H. Los sistemas de comunicación y acceso al internet se utilizan única y exclusivamente para propósitos oficiales relacionados a las funciones que realizan en el Departamento de la Familia.

I. Todos los usuarios del sistema tienen que educarse sobre los riesgos a los sistemas de virus y otros programas maliciosos, así como también sobre los procedimientos correctos para acceder la información y evitar dichas amenazas.

J. Se prohíbe utilizar el Internet para uso personal, comercial o de forma irresponsable, hostigante u ofensiva, acceder deliberadamente información, mensajes o imágenes de contenido sexual, pornográfico, obsceno o racial, y utilizar lenguaje descortés.

K. Se prohíbe acceder o instalar programas obtenidos a través del Internet, aunque sean licencias gratis, de prueba o por tiempo, salvo en aquellos casos autorizados por la OSI o el Enlace en Informática, o su representante autorizado. Además, se prohíbe utilizar el internet para copiar, acceder o enviar programas protegidos por las leyes de derecho de autor(a).

L. Los(as) usuarios(as) no deben acceder, descargar, almacenar o transmitir material que sea inapropiado para las actividades de trabajo del Departamento. Dicho material y actividades incluyen, pero no están limitadas a:

1. Páginas, portales, o como se le denomine, pornográficos de cualquier tipo
2. Páginas, portales, o como se le denomine, no relacionados al Departamento
3. *Software* y archivos no relacionados al Departamento
4. "*Chat rooms*" para la distracción personal
5. Juegos de azar

M. Los(as) usuarios(as) tienen prohibido:

1. Solicitar servicios personales o ejecutar transacciones personales, tales como: compras o verificación de cuentas personales de correo electrónico
2. Distribuir comunicaciones que puedan interpretarse como hostigamiento a otros, basados en el criterio de leyes antidiscriminatorias y política departamental.
3. Distribuir bromas, cartas o mensajes en cadena, o anuncios.
4. Esconder o representar incorrectamente su identidad al utilizar el internet.
5. Violar derechos de autor al hacer uso de material o información disponible.
6. Alterar o interferir con la intención de uso de los sistemas de información y de información de la unidad de trabajo o del Departamento de la Familia.
7. Propagar virus deliberadamente o maliciosamente.
8. Buscar para ganar acceso no autorizado a recursos de información, sistemas de información o redes dentro o fuera del Departamento.

9. Representar opiniones personales como si fueran emitidas por el Departamento.
10. Comprometer la privacidad de otros.
11. Proveer información sensitiva o confidencial de las operaciones a personas no autorizadas.

N. El Departamento no se responsabiliza por la validez, calidad, contenido o corrección de la información contenida en el Internet.

XIV. NORMAS DE USO DE REDES SOCIALES

A. Solo el personal autorizado por la Agencia podrá utilizar las redes sociales como herramienta de apoyo e información.

B. El(La) usuario(a) autorizado es responsable de sus aportaciones y de las eventuales consecuencias en su imagen y reputación.

C. Este espacio constituye un foro de intercambio de opiniones o para el debate social constructivo, pero no es el ámbito apropiado para crear polémica, descalificar a otros usuarios o a terceros, ni para presentar quejas y reclamaciones que deben canalizarse a través de las vías específicas que la Agencia tiene establecidas para esa finalidad.

D. Trate con respeto a los otros usuarios; use un lenguaje apropiado y correcto, y actúe como si estuviera en presencia de la otra persona.

E. No publique material publicitario ni haga uso del perfil para lucrarse o hacer negocio, ni compare o valore productos o servicios de otras entidades.

F. No se promocione o busque empleo a través de las redes sociales a las que fue autorizado a acceder.

G. Cualquier contribución debe presentar datos reales, concretos y argumentación consistente. Se permiten citas o la reproducción de pequeños fragmentos de textos, libros u obras en general de terceros, siempre y cuando se indique la fuente y el nombre del autor. Si realiza una contribución propia (texto, fotografías, gráficos, videos o audios), otorga a la Agencia autorización para reproducirla en

cualquier medio físico o virtual donde indicaremos su nombre como autor, y cualquier usuario también podría guardarlos o reproducirlos.

H. El logotipo del Departamento de la Familia y cualquier otro logotipo que se utilice en la cuenta del Departamento son marcas registradas. También son titularidad de la Agencia los contenidos publicados y, por tanto, la Agencia se reserva todos los derechos de propiedad intelectual e industrial asociados a los mismos.

I. Al acceder la cuenta del Departamento o a la cuenta autorizada se compromete a respetar su contenido y a no utilizarlo sin la debida autorización, cualquiera que sea el medio.

J. Desde el perfil en una red social, la Agencia no solicitará nunca las claves de acceso o firma a los sistemas, ni cualquier otra credencial personal.

K. Para el buen uso de la cuenta de red social de la Agencia, el Departamento se reserva el derecho a eliminar, sin derecho a réplica, cualquier aportación que:

1. Considere ilegal, irrespetuosa, amenazante, infundada, calumniosa, inapropiada, ética o socialmente discriminatoria o laboralmente reprochable o que, de alguna forma, pueda ocasionar daños y perjuicios materiales o morales a la Agencia, sus empleados, colaboradores o terceros.
2. Incorpore datos de terceros sin su autorización.
3. Información privilegiada o material publicitario o de propaganda, personal o en beneficio de terceros, sean personas físicas o jurídicas.
4. No esté relacionada con la finalidad de la página.

L. El Departamento de la Familia no se hace responsable de las opiniones vertidas en las cuentas de redes sociales autorizadas y no asume garantía alguna sobre la veracidad, exactitud o actualización de las informaciones en él contenidas.

M. En ningún caso, la Agencia y/o sus administradores, empleados y personal autorizado serán responsables de cualquier tipo de perjuicio, pérdidas, reclamaciones o gastos de ningún tipo, tanto si proceden como si no del uso de la red social, de la información adquirida o accedida por o a través de ésta, de virus informáticos, de fallos operativos o de interrupciones en el servicio o transmisión o fallos en la línea; el uso de esta red social, tanto por conexión directa como por

vínculo u otro medio, constituye un aviso a cualquier usuario de que estas posibilidades pueden ocurrir.

N. El Departamento de la Familia no se hace responsable de los sitios *webs* no propios a los que se puede acceder mediante vínculos ("links") desde la cuenta de red social autorizada, o de cualquier contenido puesto a su disposición por terceros.

O. El Departamento de la Familia se reserva el derecho a modificar, suspender, cancelar o restringir el contenido de este perfil, los vínculos o la información obtenida a través de ella, sin necesidad de previo aviso.

XV. ORIENTACIONES

A solicitud y en coordinación con la Secretaría Auxiliar de Planificación e Informática, el Instituto de Educación y Adiestramiento organiza y provee los recursos necesarios para llevar a cabo orientaciones, talleres, charlas o conferencias relativas a las normas sobre el uso de tecnología de información.

XVI. OFICIAL DE ENLACE

La Secretaría Auxiliar de Planificación e Informática designará un Oficial de Enlace para aclarar y/o canalizar cualquier duda que tengan los usuarios relacionada al contenido de este Manual.

XVII. ACCIÓN DISCIPLINARIA

A. Incumplir con las políticas relacionadas a los sistemas de información puede conllevar sanciones, y de ser necesario, la suspensión de los servicios recibidos.

B. Se impondrán acciones disciplinarias cuando la conducta de un(a) empleado(a) no se ajuste a las normas establecidas, utilizando la reglamentación y convenios colectivos vigentes, según corresponda. Estas se impondrán tomando en consideración el principio de disciplina progresiva.

C. La Autoridad Nominadora, en el ejercicio de su discreción, puede imponer medidas más severas, si determina que la falta cometida es de tal naturaleza o gravedad que así lo amerita.

XVIII. CLÁUSULA DE SALVEDAD

La Autoridad Nominadora es la responsable de resolver cualquier situación que no esté contemplada en este documento.

XIX. CLÁUSULA DE SEPARABILIDAD

La nulidad de alguna de las partes o disposiciones de este Manual no afectará las otras que puedan ser válidas, independientemente de las declaradas nulas.

XX. ENMIENDA

Este Manual puede ser enmendado por disposición del(de la) Secretario(a) o representante autorizado Departamento de la Familia, cuando sea necesario. Toda modificación o enmienda propuesta tiene que cumplir con los requisitos de leyes y disposiciones reglamentarias vigentes que apliquen.

XXI. DEROGACIÓN

Este Manual deroga el "Manual de Normas sobre el Uso de Tecnologías de la Información" aprobado el 3 de mayo de 2010; y cualquier otro manual, procedimiento, orden administrativa, carta circular o norma anterior que conflija con lo aquí establecido.

XXII. APROBACIÓN Y VIGENCIA

Este Manual entra en vigor a partir de la fecha de aprobación y firma por la Secretaria del Departamento de la Familia.

Idalia Colón Rondón, MTS
Secretaria

29/6/2015
Fecha

APÉNDICE 1

DEFAM – 482
SP 05/10

Estado Libre Asociado de Puerto Rico
Departamento de la Familia
Secretaría Auxiliar de Planificación e Informática
Oficina de Sistemas de Información (OSI)

DESIGNACIÓN DE REPRESENTANTE AUTORIZADO

Según requerido en el **Manual de Normas sobre el Uso de Tecnologías de la Información**, a continuación se designa al empleado o funcionario que se considerará representante autorizado:

Nombre en letra de molde del empleado o funcionario designado	**Clasificación del empleado o funcionario**
Nombre en letra de molde y firma del Secretario o Administrador	**Fecha**

Observaciones:

DESCRIPCIÓN

El formulario DEFAM-482, "Designación de Representante Autorizado", lo utiliza el Secretario o Administrador para designar a un empleado o funcionario a efectuar tareas relacionadas con el contenido del **Manual de Normas sobre el Uso de Tecnologías de Información**.

INSTRUCCIONES

Lea cuidadosamente y provea la información requerida. Si algo no aplica, favor de escribir N/A.

El formulario cuenta con un espacio para observaciones, donde el usuario puede anotar cualquier información que entienda necesaria.

La política pública del Departamento de la Familia prohíbe el discrimen de clase alguna, entre otros motivos, por género. Por lo tanto, para propósitos de este documento, todo término que se utilice al mencionar una persona o puesto se refiere a ambos géneros.

APÉNDICE 2

DEFAM-311
Oct-98

Estado Libre Asociado de Puerto Rico
DEPARTAMENTO DE LA FAMILIA

TRANSFERENCIA INTERNA DE EQUIPO

El equipo que a continuación se detalla ha sido transferido de la Oficina de

_____ a la Oficina de

_____

Fecha: _____

Número de Propiedad	Descripción	Núm. Serie

_____ Entregado por:

_____ Recibido por:

Distribución:

Original-Encargado de la Propiedad
Copia-Oficina Cedente
Copia-Receptor

El "Manual de Normas sobre el Uso de Tecnologías de la Información" se trabajó a petición de la Oficina de Sistemas de Información (OSI), adscrita a la Secretaría Auxiliar de Planificación e Informática del Departamento de la Familia. Toda pregunta o comentario sobre su contenido debe ser dirigido a la siguiente dirección postal:

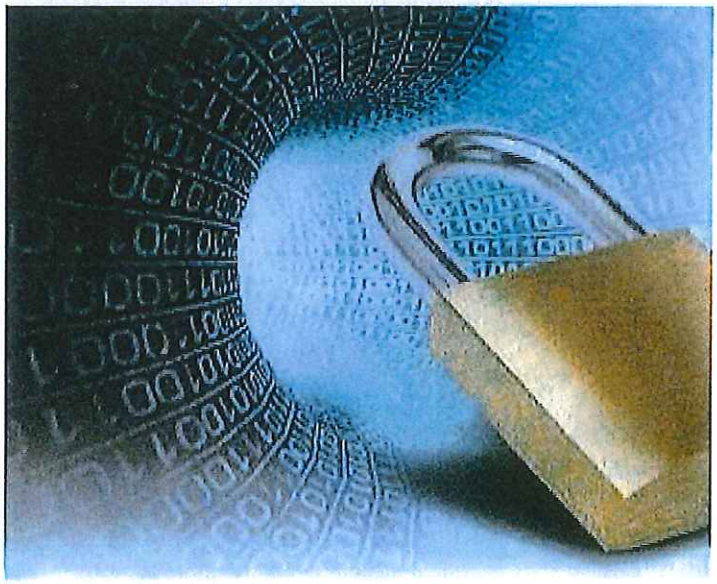
DEPARTAMENTO DE LA FAMILIA
OFICINA DE SISTEMAS DE INFORMACIÓN (OSI)
P. O. Box 11398
San Juan, Puerto Rico 00910-1398

APÉNDICE 17

MANUAL OPERACIONAL SOBRE RESGUARDO RECURRENTE DE LA INFORMACIÓN, PROGRAMAS DE APLICACIÓN Y SISTEMAS ESENCIALES

Estado Libre Asociado de Puerto Rico
DEPARTAMENTO DE LA FAMILIA
Oficina de Sistemas de Información

MANUAL OPERACIONAL SOBRE RESGUARDO RECURRENTE DE LA INFORMACIÓN, PROGRAMAS DE APLICACIÓN Y SISTEMAS ESENCIALES



Mayo 2016

MANUAL OPERACIONAL SOBRE RESGUARDO RECURRENTE DE LA INFORMACIÓN, PROGRAMAS DE APLICACIÓN Y SISTEMAS ESENCIALES

TABLA DE CONTENIDO

		Página
I.	Introducción	1
II.	Base Legal	1
III.	Propósito	2
IV.	Aplicabilidad	2
V.	Definiciones	3
VI.	Disposiciones Generales	5
VII.	Disposiciones para Servicios *Outsourcing*	9
VIII.	Cláusula de Salvedad	9
IX.	Cláusula de Separabilidad	9
X.	Enmienda	9
XI.	Derogación	10
XII.	Aprobación y Vigencia	10
	Apéndice	

I. INTRODUCCIÓN

El Departamento de la Familia reconoce la importancia de proteger y garantizar que los recursos de los sistemas de información de uso diario y crítico para sus operaciones se mantengan respaldados y sean fácilmente recuperables en el momento que sea requerido. La política pública sobre sistemas electrónicos de información es establecida por la Oficina de Gerencia y Presupuesto del Estado Libre Asociado de Puerto Rico (OGP). En su Política Núm. TIG-003 establece las directrices generales que permitirán a las agencias implantar controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y disponibilidad de la información que manejen. La sección B de dicha política requiere que las agencias tengan procedimientos para tener y mantener una copia de resguardo (*backup*) recurrente de la información y de los programas de aplicación y de sistemas esenciales e importantes para las operaciones.

La Oficina de Sistemas de Información del Departamento de la Familia establece los controles adecuados para cumplir con las directrices establecida en la Política Núm. TIG-003. A tal fin, se desarrolla este Manual para establecer el procedimiento a seguir en el Departamento de la Familia en la realización de copias de resguardo (*backup*).

II. BASE LEGAL

A. Plan de Reorganización Núm. 1 del Departamento de la Familia, según enmendado, aprobado el 28 de julio de 1995.

B. Ley Núm. 151 del 22 de junio de 2004, conocida como "Ley de Gobierno Electrónico".

C. Carta Circular Núm. 77-05 de 8 de diciembre de 2004 de la Oficina de Gerencia y Presupuesto sobre Políticas de Tecnologías de Información Gubernamental.

D. Política Núm. TIG-003, Seguridad de los Sistemas de Información, Oficina de Gerencia y Presupuesto, efectiva el 15 de diciembre de 2004 y revisada el 12 de septiembre de 2007.

E. Orden Ejecutiva del Gobernador de Puerto Rico Núm. OE-2000-19, aprobada el 12 de abril de 2000, la cual creó el cargo de Oficial Principal de Información en cada una de las agencias de la Rama Ejecutiva.

III. PROPÓSITO

El Manual tiene el propósito de establecer las normas y los procedimientos para realizar los respaldos, resguardos y recuperación de la información, programas de aplicación y sistemas esenciales del Departamento de la Familia.

IV. APLICABILIDAD

A. Las disposiciones de este Manual son de aplicación a todo el ámbito de actuación del Secretariado, sus dependencias y las Administraciones que componen el Departamento de la Familia, con excepción de la Administración para el Sustento de Menores (ASUME), de esta contar con reglamentación vigente en esta área. De no ser así entonces aplicarían las disposiciones en este manual.

B. Además, son de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual o por contrato, preste servicios a la Oficina de Sistemas de Información y en las áreas de informática de las Administraciones del Departamento de la Familia; principalmente, los responsables de los servicios de resguardo de los sistemas de información, de la generación de copias de respaldo y su ulterior recuperación, incluyendo, proveedores externos y su personal.

V. DEFINICIONES

A. **Centro de Cómputos** – Área de trabajo adscrita a la Oficina de Sistemas de Información (OSI), la cual se encarga del procesamiento de datos e información de forma sistematizada.

B. **Departamento** – Se refiere al Secretariado, sus dependencias y las Administraciones que componen el Departamento de la Familia, con excepción de la Administración para el Sustento de Menores (ASUME), de esta contar con reglamentación vigente para estas áreas.

C. **Director(a) de Sistemas de Información** – Persona responsable de planificar, organizar, coordinar, dirigir y supervisar todas las operaciones técnicas y administrativas generadas por las unidades de trabajo que integran la Oficina de Sistemas de Información.

D. **Enlace en Informática** – Título funcional de la persona encargada de administrar una red local, ofrecer apoyo tecnológico a los(as) usuarios(as) de una red, administrar contratos de servicios relacionados con la tecnología y coordinar los

asuntos relacionados a sistemas de información de un componente del Departamento (ACUDEN, ADFAN y ADSEF. Aplicará a la ASUME si su estructura así lo establece.)`

E. **Continuidad de negocios** – Se refiere a los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre, evitando así la interrupción de los servicios de críticos y necesarios para restablecer el pleno funcionamiento de las operaciones.

F. **Oficial Principal de Informática del Departamento de la Familia** – Persona designada por la Secretaria (o) que tendrá la responsabilidad de desarrollar la planificación estratégica e inversión de recursos en proyectos de informática y telecomunicaciones en el Departamento, según establecido en la OE- 2000-19 del 12 de abril de 2000.

G. **Oficina de Sistemas de Información (OSI)** – Oficina adscrita a la Secretaría Auxiliar de Planificación donde se planifican, organizan, apoyan, dirigen y supervisan las operaciones tecnológicas diarias y comunes a los componentes del Departamento; entiéndase equipos, sistemas de telecomunicaciones, correo electrónico, internet, aplicaciones, entre otros.

H. **Plan de Continuidad de Negocio** - Es un documento formal que debe ser aprobado por la Secretaria (o) del Departamento y que permite la protección de los activos (equipos, programas, datos y recursos humanos) y de las operaciones

sensitivas y críticas, en caso de eventos inesperados. Esto con el propósito de garantizar su pronto restablecimiento. El mismo debe ser parte del Plan de Manejo de Emergencias del Departamento.

I. **Resguardo (*Backup*)** – Se define como la actividad de copiar archivos, datos o datos magnéticos contenidos en un medio de almacenamiento de origen a un medio de almacenamiento alterno de forma que estén disponibles en caso de que un fallo produzca la pérdida de los archivos.

J. **Secretaria(o) Auxiliar de Planificación e Informática** – Persona designada por la Secretaria(o) para planificar, coordinar, dirigir, supervisar y evaluar todas las actividades que se desarrollan en las oficinas adscritas a la Secretaría Auxiliar de Planificación e Informática, entre estas la Oficina de Sistemas de Información. Participa activamente en la formulación de la política pública de su área de trabajo y en la dirección y supervisión de los proyectos estratégicos de tecnología del Departamento de la Familia.

K. **Sistemas** – Conjunto de aplicaciones, programación, información, equipos de telecomunicaciones, servidores y periféricos que se utilizan para la recopilación, almacenamiento, análisis, gerencia, control e intercambio de datos.

VI. DISPOSICIONES GENERALES

A. Toda la información importante y crítica para la continuidad de negocios será periódicamente respaldada en soportes de *backup*.

B. Las copias de *backup* deben abarcar toda la información necesaria para recuperar el servicio en caso de corrupción o pérdida de la información. Tal información puede incluir datos, programas, ficheros de configuración e incluso imágenes de los sistemas operativos.

C. En relación con los archivos de datos, se recomienda mantener al menos tres generaciones de respaldos. De éstas, se debe mantener una copia almacenada en un lugar seguro fuera del edificio donde están instalados los servidores principales, y que sea una localidad que ofrezca las condiciones ambientales y de seguridad necesarias. El acceso de personas a estos medios será restringido y controlado.

D. El Director(a) de Sistemas de Información y los Enlaces en Informática establecerán los ciclos de copia más adecuados para los sistemas relevantes y definirán los estándares y procesos de resguardo, que incluirán, al menos, la siguiente información:

1. Los aplicativos y/o bases de datos y servidores que se les hará copias de *backup*.
2. Herramienta de resguardo y las versiones.
3. Tipo y periodicidad de los *backup*
4. Periodos de retención de las copias.
5. Ubicación de los *backup*.
6. Procedimientos de recuperación de la información.

7. Procedimientos de restauración y verificación de la integridad de la información resguardada.

8. Procedimientos de inventario y gestión de soportes.

E. Los procesos establecidos en el inciso D estarán documentados y regulados. A tal fin, el Director de la Oficina de Sistema de Información preparará y mantendrá una o varias carpetas con la documentación esencial para realizar resguardos eficientes de la data, programas de aplicación y sistemas críticos. La documentación será clara, completa y correcta en cada etapa, desde el desarrollo hasta la operación del *backup*, y debe revisarse anualmente o actualizarse inmediatamente haya un cambio en el proceso. Ver Apéndice 1.

También, se incluirán las rutinas de las herramientas utilizadas para realizar el *backup* y toda la información técnica y necesaria sobre las herramientas y servidores de *backup*.

Esta información deberá ser revisada y actualizada anualmente o tan pronto ocurra cualquier incidente que requiera nuevas herramientas, añadir operaciones o servidores críticos al resguardo, así como cambios a las políticas y procesos establecidos

F. Se deberá llevar un registro (*log*) de problemas en las rutinas de *backup* para facilitar el proceso de solución.

G. El Director de la Oficina de Sistemas de Información preparará o mantendrá actualizado anualmente un Plan de Continuidad de Negocios que permita la

protección de los activos (equipos, programas, datos y recursos humanos) y de las operaciones sensitivas y críticas, en caso de eventos inesperados. Esto con el propósito de garantizar su pronto restablecimiento. El Plan debe ser aprobado por la Secretaria (o) del Departamento y formará parte del Plan de Manejo de Emergencias del Departamento.

H. El Plan debe proveer, entre otras cosas, lo siguiente:

1. Las responsabilidades del personal asignado al área de Sistemas de Información durante y después de ocurrida la emergencia.
2. Las responsabilidades de cada empleado al momento de ponerse en ejecución el plan.
3. Una relación del personal clave, sus direcciones y números de teléfono donde pueden ser localizados.
4. Procedimientos de desalojo del área de Sistemas de Información con orientación al personal sobre las salidas de emergencia.
5. Procedimientos para la utilización de los respaldos del equipo, de los programas, de los archivos y de la documentación.
6. Una relación con los nombres, las direcciones y los números de teléfono de proveedores de equipo, programas y materiales.
7. Los arreglos con otros centros de cómputos para el procesamiento y ejecución de los programas.

8. Procedimientos para mantener actualizado el Plan de Continuidad de Negocios.

VII. DISPOSICIONES PARA SERVICIOS *OUTSOURCING*

Todo servicio subcontratado que maneje información, programas de aplicación y sistemas críticos y esenciales del Departamento de la Familia tiene que contar con un proceso de resguardo que permita la continuidad de negocios.

VIII. CLÁUSULA DE SALVEDAD

La Autoridad Nominadora es la responsable de resolver cualquier situación que no esté contemplada en este documento.

IX. CLÁUSULA DE SEPARABILIDAD

La nulidad de alguna de las partes o disposiciones de este Manual no afectará las otras que puedan ser válidas, independientemente de las declaradas nulas.

X. ENMIENDA

Este Manual puede ser enmendado por disposición del(de la) Secretario(a) o representante autorizado(a) del Departamento de la Familia, cuando sea necesario. Toda modificación o enmienda propuesta tiene que cumplir con los requisitos de leyes y disposiciones reglamentarias vigentes que apliquen.

XI. DEROGACIÓN

Este Manual deroga cualquier otro manual, procedimiento, orden administrativa, carta circular o norma anterior que conflija con lo aquí establecido.

XII. APROBACIÓN Y VIGENCIA

Este Manual entra en vigor a partir de la fecha de aprobación y firma por la Secretaria del Departamento de la Familia.

Idalia Colón Rondón, MTS
Secretaria

17 mayo 2016
Fecha

APÉNDICE

APÉNDICE 1

ESTÁNDARES Y PROCESOS DE RESGUARDO[1]

I. HERRAMIENTA

A. La herramienta que se utiliza para realizar resguardo es el programa especializado "Symantec Backup Exec", versión 12.5, con cliente para resguardar Exchange, SQL y "Systems State".

B. Las copias de seguridad son almacenadas en el "data storage" configurado en el servidor SECBACKUP con capacidad de almacenamiento de 2.4 TB (Terabyte).

C. Todos los días cotejarán si los resguardos se ejecutaron correctamente.

D. Por lo menos, cada tres meses se hacen ejercicios de "restore" de servidores, bases de datos y documentos. De haber alguna cancelación de algunos o todos los "backups" antes mencionados, se envía un correo electrónico con la DEFAM-521, Hoja de Control de Cambios para Sistemas de Información, al Director de la Oficina de Sistemas de Información donde se establecerá la acción correctiva. Apéndice 1-A

E. Todo cambio al "Backup Exec" 12.5 debe ser informado a los responsables del resguardo de información, quienes son:

   A. Sr. José R. Flores, Supervisor de Operaciones – Responsable

   B. Sr. Alberto Cappa, Administrador de Red – Sustituto

   Estos deberán documentar la situación en casos de cancelación y creación de reglas nuevas de resguardo con un "print screen", el cual refleje "backups" cancelados. Además, deben documentar la situación, verificar por qué ocurrió, realizar acción correctiva e informar al Director.

[1] Este documento debe ser enmendado cada vez que surjan cambios, de manera que la información esté actualizada.

II. DESCRIPCIÓN DE TAREAS Y CONFIGURACIÓN DE LA HERRAMIENTA DE "BACKUP"

La herramienta de "Backup Exec 12.5" es un programa desarrollado por Symantec Corp., el cual provee una solución centralizada para realizar las respectivas copias de seguridad, ya sea en ambiente físico o virtual. Con la información, según detallada, se pretende ilustrar detalles técnicos en el ambiente del servidor, detalles técnicos en el ambiente software "Backup Exec 12.5", condiciones generales, políticas configuradas, procedimientos y rutinas para el resguardo de la información.

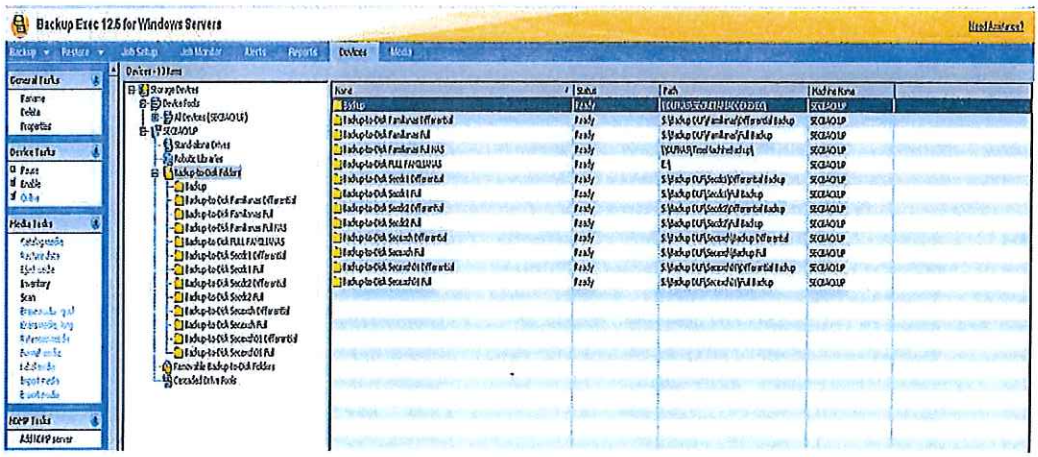
A. Detalles Técnicos del Ambiente Servidor Departamento de la Familia

Etiqueta	Valor predeterminado y descripción
Servidor	*HP ProLiant DL380 G6*
Hardware	**8 CPU** x 2GHz Intel ® Xeon E5504 (a) / **RAM**: 73717.28 MB / **Data Store** 2.4 TB
Software	**Windows Server 2008 R2 Enterprise Service Pack 1**

B. Detalles Técnicos, Ambiente *Backup* Departamento de la Familia

Etiqueta	Valor predeterminado y descripción
Software	Symantec Backup Exec 12.5
Media Server	Version 12.5 Rev. 2213
Administration Console	Version 12.5 Rev. 2213

C. Condiciones Generales, Políticas y Rutinas Configuradas *Backup Exec* 12.5



D. DESCRIPCIÓN DE SERVIDORES Y EL MÉTODO DE *BACKUP* A SER UTILIZADO

symantec. **Device Usage By Policy**

Familianas Backup

Backup-to-Disk Familianas Differential

Template Name	Method
Familiana Daily Backup	DIFFERENTIAL - Changed Files, Reset Archive Bit

Familianas Backup

Backup-to-Disk Familianas Full

Template Name	Method
Familianas Backup	FULL - Backup Files - Reset Archive Bit

SECDC Backup

Backup-to-Disk Secdc1 Differential

Template Name	Method
Daily Backup	DIFFERENTIAL - Changed Files, Reset Archive Bit

SECDC Backup

Backup-to-Disk Secdc1 Full

Template Name	Method
Weekly Backup	FULL - Backup Files - Reset Archive Bit

SecExch Backup

Backup-to-Disk Secexch Differential

Template Name	Method
Daily Backup	DIFFERENTIAL - Changed Files, Reset Archive Bit

SecExch Backup

Backup-to-Disk Secexch Full

Template Name	Method
Weekly Backup	FULL - Backup Files - Reset Archive Bit

Report Date: 2/26/2016 10:05:28 AM

This report was generated by Symantec Backup Exec. Symantec Backup Exec is a registered trademark of Symantec Corporation. Other trademarks are the property of their respective owners.

Page 1

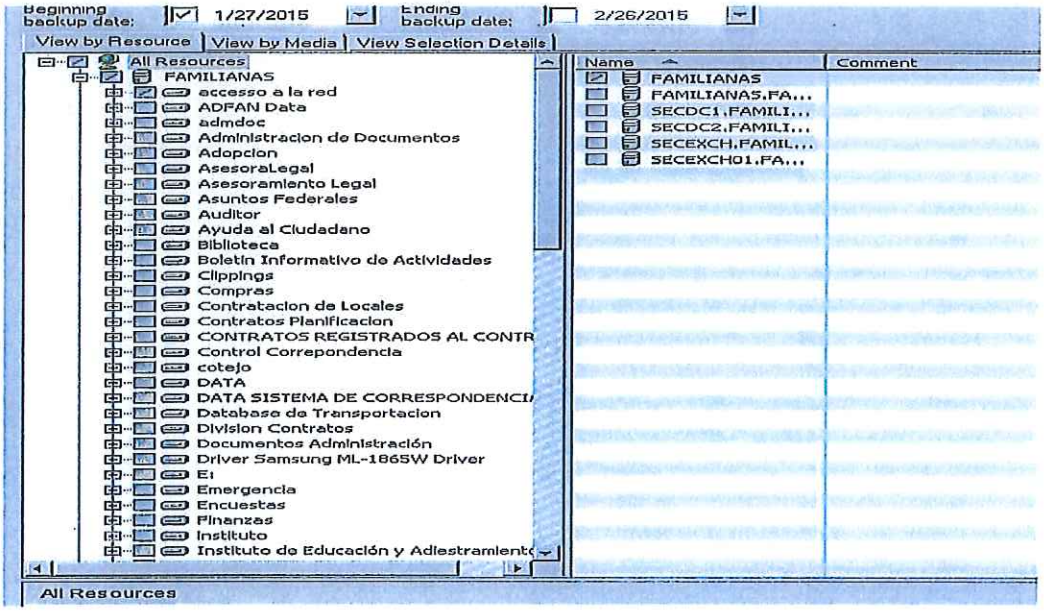
III. INFORMACIÓN RESPALDADA - ESQUEMA SECRETARIADO, OFICINA CENTRAL

Los servidores que proveen los servicios más críticos se identifican tomando como base la información acumulada y la garantía de la continuidad de la operación. La información a continuación describe el nombre de cada servidor y la descripción del servicio que estos ofrecen:

	Servidor	Descripción
A.	FAMILIANAS	Repositorio de Usuarios y Base de Datos Aplicativos.
B.	SECEXCH	Mail Box – Base de datos Correo Electrónico
C.	SECEXCH01	Mail Box – Base de datos Correo Electrónico
D.	SECDC1	Esquema de Active Directory Dominio Familia
E.	SECDC2	Esquema de Active Directory Dominio Familia

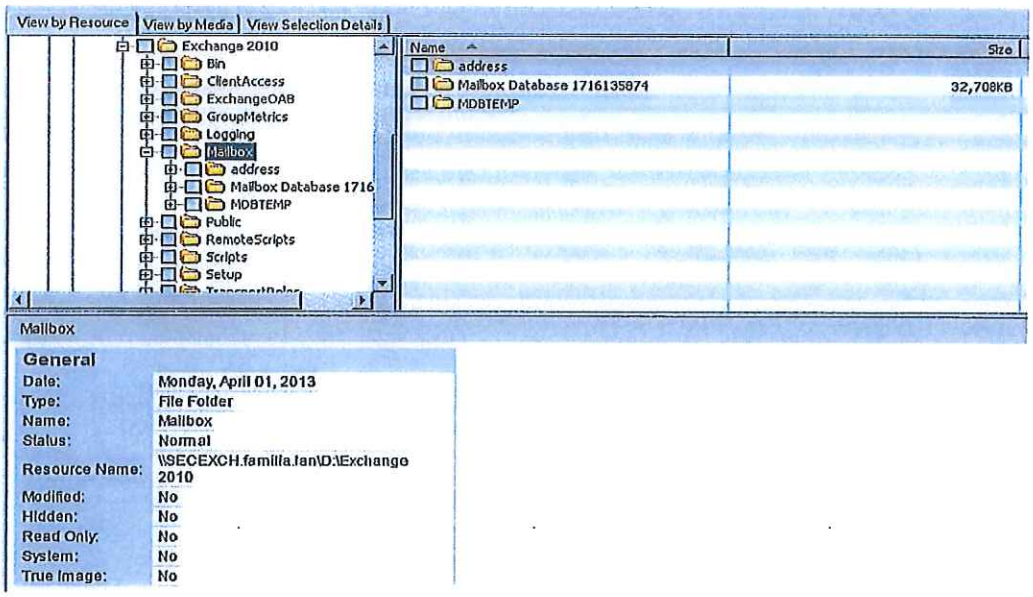
A. Ambiente Servidor FAMILIANAS

El Servidor FAMILIANAS tiene la función de "file server", el cual provee a los usuarios un repositorio para el almacenamiento de información generada por estos. Esta información se almacena en carpetas identificadas con la nomenclatura alusiva a la oficina y nombre del usuario. Todos los repositorios provisionados en este servidor son respaldados por una rutina de resguardo de "Backup Exec 12.5". En la siguiente ilustración, se muestra lo antes expuesto:



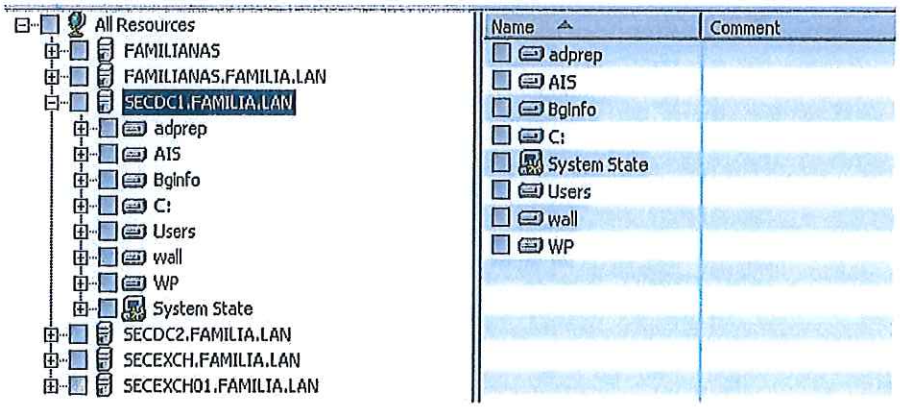
B. Ambiente Servidor de Correo SECEXCH y SECEXCH01

El Servidor de Correo SECEXCH y SECEXCH01 tiene como función el proveer el servicio de mensajería electrónica, administrada y manejada por Microsoft Exchange 2010. Todos los "mailbox" de los usuarios del Secretariado Nivel Central se encuentran en estos servidores. El "Backup Exce 12.5" tiene una rutina configurada que respalda las bases de datos de ambos servidores según muestra la siguiente imagen:



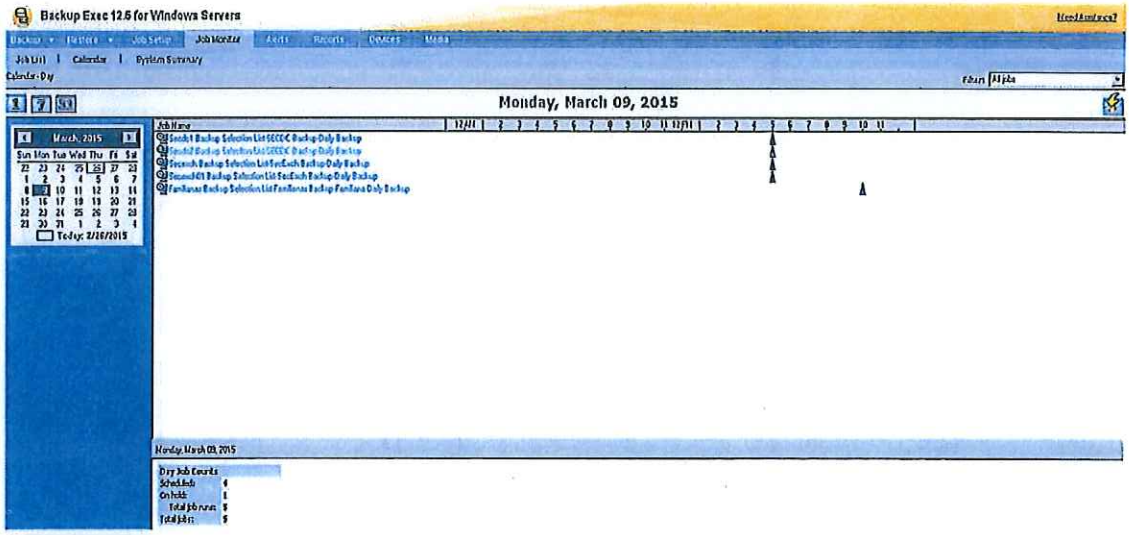
C. **Ambiente "Domain Controler" Principal SECDC1 y Secundario SECDC2**

Los ambientes SECDC1 y SECDC2 ofrecen la función de controladores de dominio. Esta función se realiza a través de "Microsoft Active Directory", ambiente "Windows Server 2008 R2". La información relacionada a cuentas de usuarios y políticas aplicadas "Group Policy" es respaldada mediante una rutina configurada en "Backup Exec 12.5":

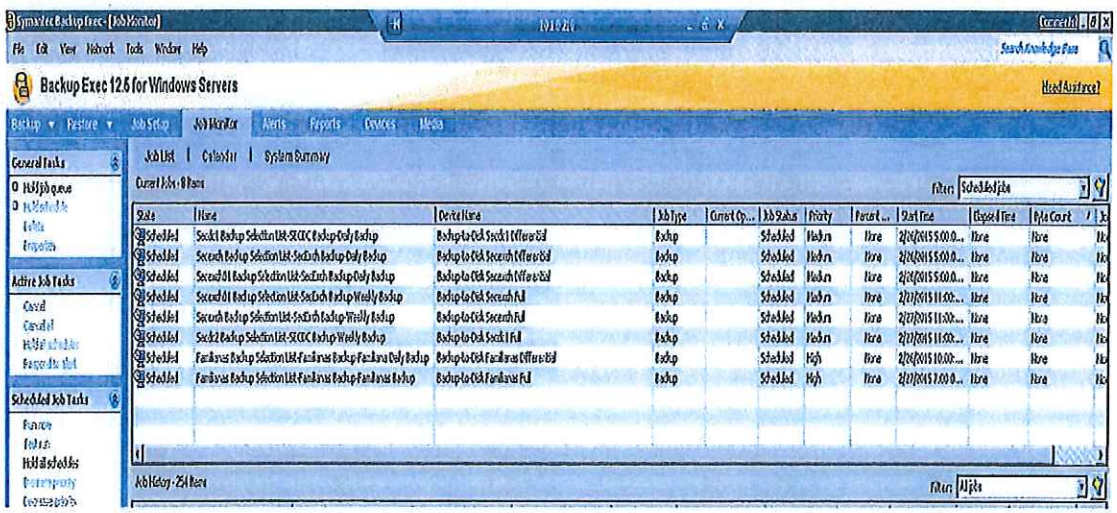


IV. PROCEDIMIENTO PARA EL RESGUARDO DE LA INFORMACIÓN Y LAS RUTINAS CALENDARIZADAS SECRETARIADO, OFICINA CENTRAL

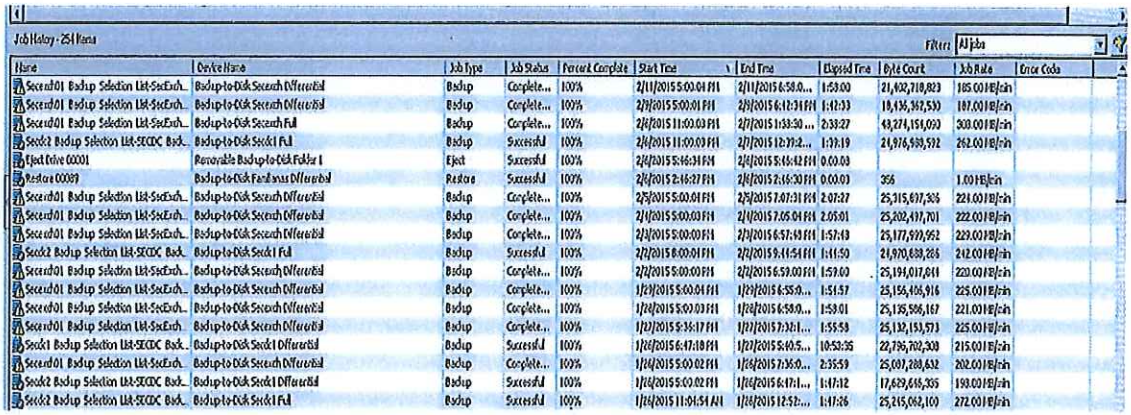
El procedimiento para el resguardo de la información consiste en rutinas automatizadas programadas diariamente o semanal. Diariamente, las rutinas que se ejecutan comienzan a partir de las 5:00 pm y no tienen orden de prioridad. Estos "backups" son diferenciales de lunes a jueves y apoyados en los "full backups" que se realizan los fines de semana.



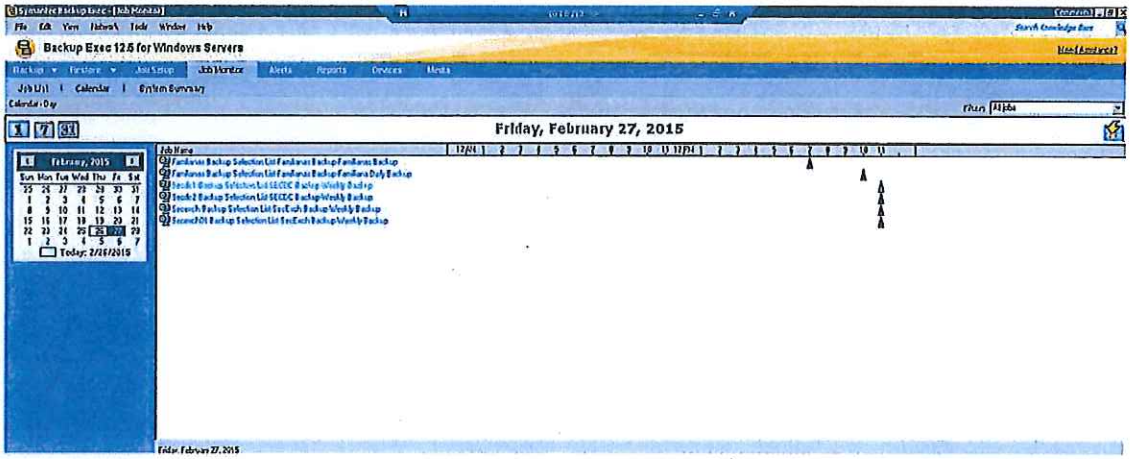
En la siguiente ilustración se muestra el itinerario de los "backups" diferenciales según configurados.



Una vez completado cada "backup", se genera un registro de estatus o "Job History Items". Utilizando este mecanismo se puede identificar si ocurrió una falla en el proceso y de esta manera se inicia el proceso para remediar la situación.



Las rutinas programadas para el fin de semana "Full Backup" comienzan a partir de las 7:00 pm los viernes de cada semana. Estas rutinas, al igual que el ambiente diferencial, no tienen definido un orden de prioridad por lo que el mismo sistema es quien decide qué rutina inicia.

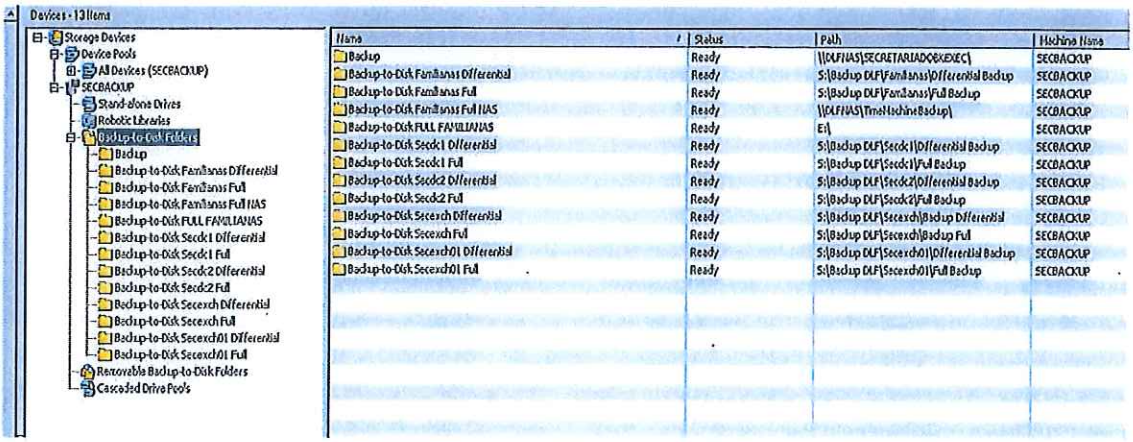


V. DETALLES DE ALMACENAMIENTO "MEDIA SERVER" "BACKUP EXEC 12.5" SECRETARIADO, OFICINA CENTRAL

A. Todas las copias de seguridad son almacenadas en el "data storage" configurado en el servidor SECBACKUP.

B. La capacidad de almacenamiento es de 2.4 TB y no se establece cuota en ninguna de las rutinas.

C. Cada rutina tiene creada una carpeta con la nomenclatura alusiva a la rutina.



El "Manual Operacional sobre Resguardo Recurrente de la Información, Programas de Aplicación y Sistemas Esenciales" se trabajó a petición de la Oficina de Sistemas de Información del Secretariado del Departamento de la Familia. Toda pregunta o comentario sobre su contenido debe ser dirigido a la siguiente dirección postal:

DEPARTAMENTO DE LA FAMILIA
OFICINA DE SISTEMAS DE INFORMACIÓN
P O BOX 11398
SAN JUAN PR 00910-1398

* * *

Este documento estará disponible en formato digitalizado en la Oficina de Sistemas y Procedimientos. Puede comunicarse con el personal de esta Oficina a través del 787-294-4908.

APÉNDICE 18

REGISTRO DE INCIDENCIAS EN PROCESOS DE RESGUARDO DIARIO

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Departamento de la Familia

REGISTRO DE INCIDENCIAS EN PROCESOS DE RESGUARDO DIARIO

Fecha	Hora	¿Hubo Incidencia?		Situación Identificada	Acción Tomada	Nombre del Técnico	Firma
		Sí	No				

Oficina de Sistemas de Información
Edif. Lila Mayoral, 306 Ave Barbosa
PO Box 11398, San Juan, PR 00910-1398
Tel. 787.625.4900 Exts.: 1008 y 1073

DEPARTAMENTO FAMILIA
Estado Libre Asociado de Puerto Rico

El "Plan de Seguridad de los Sistemas de Información" se trabajó a petición de la Oficina de Sistemas de Información (OSI) de la Secretaría Auxiliar de Planificación e Informática. Toda pregunta o comentario sobre su contenido debe ser dirigido a la siguiente dirección postal:

DEPARTAMENTO DE LA FAMILIA
SECRETARÍA AUXILIAR DE PLANIFICACIÓN E INFORMÁTICA
OFICINA DE SISTEMAS DE INFORMACIÓN
P O BOX 11398
SAN JUAN PR 00910-1398

* * *

El Plan y los formularios del Departamento (DEFAM) estarán disponibles en formato electrónico en la Oficina de Sistemas y Procedimientos. Puede comunicarse con el personal de esta Oficina a través del 787-294-4908.