Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: TI-15-01 Número de unidad: 5386 Nombre de la entidad auditada: Negociado de la Policía de Puerto Rico, Negociado de Tecnología y Comunicaciones, División de Tecnología

Fecha del informe de auditoría o especial: 14 de octubre de 2014 Período auditado: 8 de octubre de 2012 al 31 de agosto de 2013

Indique el informe que remite: ☐ **PAC** ☒ **ICP -** 12 Indique si incluye anejo/s: ☐ Sí ☒ No

Funcionario de enlace: Myriam Y. Rivera Rodríguez Puesto: Auditora Teléfono: 787-903-5602, ext. 6014

Funcionario principal o su representante autorizado: Elmer L. Román González Puesto: Secretario Teléfono: 787-903-5602, ext. 6005

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 13/mayo/19
Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
Asegurarse de que se realicen las gestiones necesarias para que se prepare un plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones. Este plan debe ser remitido para revisión y aprobación. Una vez este sea probado, tomar las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la Policía. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 3-a: Recomendación 4]**	El Director del NTC del Negociado de la Policía de Puerto Rico (NPPR), presento el Plan de Continuidad de Negocios de dicho Negociado, debidamente aprobado. Se incluye copia del Plan de Continuidad, para su evaluación.	Negociado de Tecnología y Comunicaciones (NTC) y Oficina Legal	Abril 2019	**Cumplimentada**

(Véanse instrucciones al final).

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: TI-15-01 Número de unidad: 5386 Nombre de la entidad auditada: Negociado de la Policía de Puerto Rico, Negociado de Tecnología y Comunicaciones, División de Tecnología

Fecha del informe de auditoría o especial: 14 de octubre de 2014 Período auditado: 8 de octubre de 2012 al 31 de agosto de 2013

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN

(Véanse instrucciones al final).

INSTRUCCIONES PARA COMPLETAR Y REMITIR EL PLAN DE ACCIÓN CORRECTIVA

Instrucciones:

1. Este documento debe estar completado en todas sus partes.

   a. La primera página debe contener, entre otra información: el número y la fecha del informe de auditoría o especial relacionado; indicación sobre el documento que se remite (*PAC* o *ICP*); el nombre del funcionario de enlace y del funcionario principal; y la firma del funcionario principal o su representante autorizado.

   b. En las columnas se requiere la siguiente información:

      1) **Recomendación**: En esta columna se detallan las recomendaciones. Las recomendaciones se presentan en el mismo orden y con el número de identificación que aparece en el informe de auditoría o especial.

      2) **Acción Correctiva**: En esta columna se indican las medidas adoptadas o las que adoptarán para corregir las situaciones señaladas y eliminar las causas de estas. Las acciones correctivas deben ser alcanzables y diseñadas para prevenir que las situaciones se repitan.

      3) **Persona o área responsable**: En esta columna se identifica/n el/los funcionario/s o el/las área/s responsable/s de implantar las acciones correctivas.

      4) **Fecha de implantación**: En esta columna se indica la fecha probable para cumplir con las acciones correctivas.

      5) **Estatus de la recomendación**: En esta columna se indica el nivel de cumplimiento de la recomendación. Esto es:

         - **Cumplimentada**: Recomendaciones para las cuales se tomaron acciones correctivas y se obtuvieron los resultados deseados.
         - **Parcialmente cumplimentada**: Recomendaciones para las cuales se han establecido medidas correctivas, pero quedan algunos asuntos pendientes.
         - **No cumplimentada**: Recomendaciones para las cuales no se han establecido acciones correctivas.

      En cada una de los columnas descritas en el apartado del **b.2) al 5)** de esta instrucción se deben ofrecer datos que permitan una evaluación adecuada. Si se objeta alguna recomendación, se deben incluir las razones y una descripción específica de la/s acción/nes correctiva/s alterna/s.

2. Cuando el funcionario principal delegue la función de certificar este documento, antes de remitir el mismo, debe notificar por escrito a la dirección de correo electrónico AdminPAC@ocpr.gov.pr el nombre y el puesto del funcionario en quien delegó la misma.

3. El documento digitalizado debe remitirse a la Oficina mediante la aplicación *Sistema Plan de Acción Correctiva* que esta creó para estos propósitos[1]. Esto, dentro del término de 90 días consecutivos, contados a partir del primer día del mes siguiente a la fecha de publicación del informe de auditoría o el especial. Cuando queden recomendaciones pendientes de cumplimentar, a la fecha del primer informe, se prepararán informes complementarios *(ICP)* cada 90 días, contados a partir del primer día del mes siguiente a la fecha de la notificación del resultado de la evaluación. El envío debe ser en la forma indicada anteriormente.

4. Los documentos que se utilicen para justificar las acciones correctivas informadas deben estar disponibles para examen por esta Oficina.

---

[1] La aplicación *Sistema Plan de Acción Correctiva* v1.0 está localizada en nuestra página en Internet: www.ocpr.gov.pr bajo la sección Contraloría Digital. Si no tiene una cuenta registrada en dicha aplicación envíe un correo electrónico a AdminPAC@ocpr.gov.pr para solicitar información de cómo registrar una cuenta en la misma.

GOBIERNO DE PUERTO RICO

Negociado de la Policía de Puerto Rico

PLAN DE CONTINUIDAD DE NEGOCIOS DE LA DIVISIÓN DE TECNOLOGÍA

Aprobado:

Henry Escalera Rivera
Comisionado

ABRIL 2019

I. OBJETIVOS:

El Plan de Continuidad de negocios implica un análisis de los posibles riegos tecnológicos del Negociado de la Policía de Puerto Rico, a los cuales pueden estar expuestos los sistemas computadorizado y la información contenida en los diversos medios de almacenamiento.

El objetivo principal de este plan es garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.

Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

Restaurar el Servicio de Cómputo en forma rápida, suficiente y con el menor costo y pérdidas posibles antes cualquier eventualidad.

II. PROPÓSITO

El propósito de este plan es mantener la continua ejecución de los procesos de misión crítica y sistemas de información tecnológica del NPPR, en el caso extraordinario que un evento pudiera ocasionar que los sistemas fallen en el mínimo de su producción.

El Plan de Continuidad de Negocio del NPPR contiene las necesidades y requerimientos de tal forma que el NPPR pueda estar preparado para responder a un evento y, en su caso, hacer eficiente la restauración de los sistemas que hayan estado inoperables por el evento.

III. ALCANCE

El plan de continuidad de negocios que se desarrolla en el presente documento es de aplicación a todas las áreas funcionales en la estructura orgánica de tecnología del Negociado de la Policía de Puerto Rico.

IV. BASE LEGAL

1. Esta política está desarrollada conforme al Acuerdo para la Reforma Sostenible del NPPR, en el Área de Cumplimiento de Sistemas de información y Tecnología (Sección XIII, Requerimientos 218 al 224).
2. Orden General Capitulo 400, Sección 403, titulada: Normas para el Uso de los Sistemas Computadorizados (OG 403).

3. Manual para la Administración de los Sistemas Computadorizado del NPPR.
4. POLITICA NÚM. TIG-003, Seguridad de los Sistemas de Información. REVISIÓN: 12 de septiembre de 2007 de TECNOLOGIAS DE INFORMACION GUBERNAMENTAL, OFICINA DE GERENCIA Y PRESUPUESTO.

V. DEFINICIONES

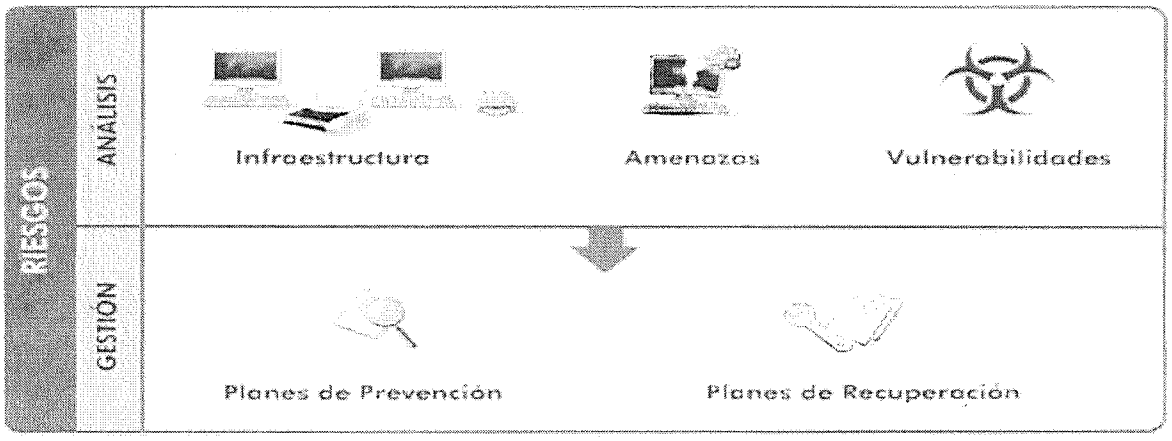
1. **NPPR:** Negociado de la Policía de Puerto Rico.
2. **Activo de información:** Es cualquier elemento que tenga valor para el NPPR y, en consecuencia, debe ser protegido.
3. **Amenaza:** Factor externo que aprovecha una debilidad en los activos informáticos y puede impactar en forma negativa al NPPR. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.
4. **Contención:** Evitar que el incidente siga ocasionando daños.

VI. PLAN DE CONTINUIDAD DE NEGOCIO.

Este plan es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y las Comunicaciones. Dicho plan contiene las **medidas técnicas, humanas y organizativas** necesarias para garantizar la continuidad de las operaciones de la Agencia.

Así mismo, este plan sigue el conocido ciclo de vida interactivo "**PLAN-DO-CHECK-ACT**", es decir, "planifica-actúa-comprueba- corrige". Surge de un análisis de riegos del Negociado de la Policía de Puerto Rico, donde entre otras amenazas, se identifican aquellas que afectan la continuidad de la operación en la Agencia.

El Plan de Continuidad de Negocios deberá ser revisado y/o evaluado semestralmente, o cuando se materialice una amenaza.



El plan de continuidad de negocios incluye de cuatro planes:

1. **Plan de respaldo.**

   Contempla las medidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

2. **Plan de emergencia.**

   Contempla las medidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es contrarrestar los efectos adversos de la misma.

3. **Plan de recuperación.**

   Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

4. **Plan en caso de temporada ciclónica.**

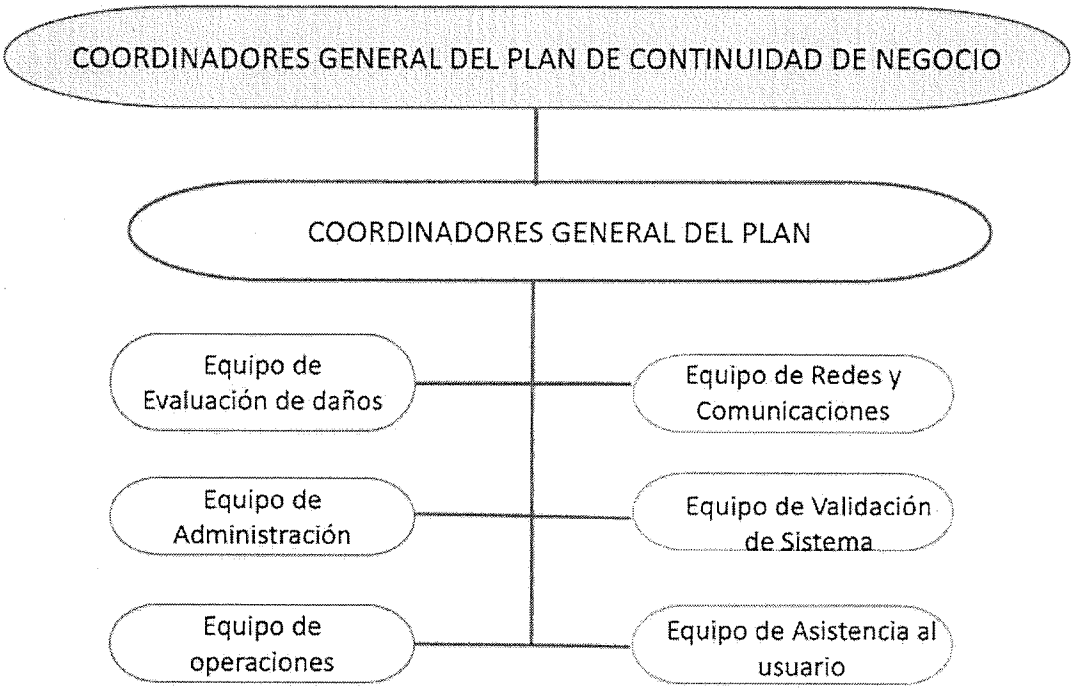
   Incorpora las acciones, responsables y actividades en caso de una amenaza de huracán. (Ver Anejo A).

VII. ORGANIZACIÓN

En el caso de un desastre u otra circunstancia que conlleve la necesidad de operaciones de contingencia, la operación normal de la Agencia deberá cambiar a una operación de contingencia. El NPPR deberá centrarse en cambiar, la estructura actual y funciones de un "día normal de trabajo", a la estructura y funciones requeridas por la contingencia trabajando en conjunto para la restauración en tiempo de las operaciones normales de la misma.

A continuación, se presenta la estructura propuesta en el siguiente diagrama:

COORDINADORES DEL PLAN DE CONTINUIDAD DE NEGOCIO DE TECNOLOGIA
DIVISION DE TECNOLOGIA



VIII. Fase del Plan de Continuidad.

El Coordinador del Plan del NPPR, en conjunto con sus directivos, determinara cuáles equipos y miembros son responsables de cada función durante las fases:

1. Fase de Respuesta
2. Fase de Reasunción
3. Fase de Recuperación
4. Fase de Restauración

IX. Sistemas/Aplicaciones/Servicios de Misión Crítica

Los siguientes sistemas/aplicaciones/servicios de misión crítica deberán ser recuperados en el caso de un desastre:

Acrónimo del Sistema	Nombre del Sistema
LAN	Conexión de Red Interna
WAN	Conexión de Red Externa
DNS	Servicio de Resolución de Nombres

Acrónimo del Sistema	Nombre del Sistema
Correo	Sistema de Correo Electrónico
BD	Base de Datos
DC	Controladores de Dominio

X. AMENAZAS

La siguiente tabla muestra las amenazas más comunes que podrían impactar la continuidad y componentes de sistemas y su administración. Las amenazas que son presentadas con (**XX**) son consideradas las de mayor probabilidad de ocurrir.

PROBABILIDAD DE AMENAZAS			
Probabilidad de ocurrencia:	**Alta**	**Media**	**Baja**
Falla del aire acondicionado		XX	
Accidente aéreo			X
Chantaje		X	
Amenazas de bomba			X
Pérdida de comunicación		X	
Destrucción de información		X	
Terremotos			X
Fuego			X
Inundación / Daño por agua			X
Corte eléctrico /interrupción	X		
Sabotaje / Terrorismo			X
Tormentas / Huracanes	XX	X	
Vandalismo			X

XI. PLAN DE CONTINUIDAD PARA EL SUMINISTRO DE ENERGÍA ELÉCTRICA EN EL CENTRO DE COMPUTOS PRINCIPAL UBICADO EN EL CUARTEL GENERAL DEL NPPR.

A. Acciones Preventivas a la Contingencia

1. Planta de Emergencia

a. El Centro de Cómputos está integrado a la planta de emergencia principal del edificio la cual suministra energía regulada a todos los equipos existente en el Centro de Cómputos del NPPR.
b. Supervisar semanalmente el nivel óptimo de combustible, agua, baterías, etc. (Persona de Edificio Publico realiza el mantenimiento correspondiente a planta de emergencia).
c. Contar con un plan de mantenimiento semestral con supervisiones mensuales.

d. Supervisar el combustible de respaldo en el área de Edificio Público.
e. Contar con equipo de emergencia contra incendios en el local de la planta
f. Contar con el mapa eléctrico del área en la planta y archivado, identificando los contactos respaldados y regulados (Edificio Público es el responsable de esta tarea)
g. Edificio Publico cuenta con un procedimiento de operación y uno en caso de un mal funcionamiento de la planta de emergencia.

2. Sistema eléctrico de alimentación ininterrumpida "UPS"

a. Nuestro Centro de Computo cuenta con un UPS redundante con las capacidades necesarias (40% superiores).
b. Plan de mantenimiento anual integral con supervisiones mensuales
c. Contar con el mapa eléctrico del área, identificando los contactos regulados y respaldados.
d. Contar con un procedimiento de operación y uno en caso de un mal funcionamiento.
e. Determinar semestralmente el tiempo efectivo y real de respaldo del UPS con respecto a las diferentes cargas.

3. Generales

i. Contar con un directorio de los responsables del suministro eléctrico en cada nodo.
ii. Contar con un procedimiento para reportar el incidente a las áreas involucradas (**Edificio Públicos, PRTC (Claro), INTECH, etc.**).
iii. Contar con un procedimiento para notificar a los usuarios afectados la probable baja de los servicios de comunicación.
iv. Contar con procedimiento de ejecución de respaldos de emergencia a la información de las aplicaciones y sistemas críticos.
v. Contar con una tabla de claves de prioridades para dar aviso a los usuarios prioritarios con el fin de optimizar tiempo y recursos.
vi. Solicitar revisión periódica (semestral) del estado y óptimo funcionamiento de los bancos de respaldo eléctrico en los equipos del proveedor de medios.
vii. Asignar jerarquía a los equipos Activos y Servicios para ejecutar medidas mayores (darlos de baja).
viii. Determinar las fases de una contingencia de esta índole.

4. Acciones Durante el plan por interrupción del sistema eléctrico.

a. En caso de interrupción del suministro eléctrico del sistema público pero la planta de emergencia del edificio funcionando:

i. Comunicarse con el personal destacado de Edificio Público para la supervisión de la Planta de emergencia
ii. Monitorear el UPS cada 20 min. para programar acciones mayores
iii. Valorar la decisión de dar de baja los equipos activos y/o servicios menos prioritarios para evitar daños y/o pérdida de información y de equipos y aumentar la capacidad de duración de las baterías del UPS.

b. En caso de interrupción del suministro eléctrico del sistema público y la planta de emergencia del edificio fuera de servicio:

i. Comunicarse con el personal destacado de Edificio Público para la supervisión de la Planta de emergencia.
ii. Monitorear el UPS cada 10 min. para programar acciones mayores
iii. Apagar los equipos no prioritarios como impresoras, monitores o Servidores que no demanden su uso.
iv. Contar con los procedimientos para dar de baja (Shutdown) los equipos activos en caso de que la planta de emergencia no entre en función y el UPS tenga 30% de energía en reserva.
v. Dar aviso de la contingencia a las siguientes áreas de trabajo:
   a) Oficina del Comisionado, Comisionado Auxiliares (Operaciones de Campos, Servicios Gerenciales, Responsabilidad Profesional e investigaciones Criminales.
   b) Proceder a desactivar los servidores (Shutdown) en el siguiente orden:

Tabla de Servidores en orden de apagado

Falla del Sistema Eléctrico Público, en función el Sistema de Planta de Emergencia

Nombre	Modelo	Sistema Operativo	Descripción
Policia01	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Sistema De Asistencia De Laboratorio
Policia02	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Enterprise	Sistema De Asistencia De Laboratorio
Policia03	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	File Server

Nombre	Modelo	Sistema Operativo	Descripción
Policia04	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	File Server
Policia5	VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Standard Edition	Sistema De Nomina Histórico
Policia06	VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Standard Edition	Data Base Server & File Server
Policia07	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	Data Base Server & File Server
Policia08	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Data Base Server Sistema Asistencia
Policia09	VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Standard Edition	Data Base Server & File Server
Policia10	VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Standard Edition	Data Base Server de Anpe
Policia11	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	App Server Sistema Asistencia
Policia12	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	File Server (Cradic)
Policia13	VMware Virtual Platform	Microsoft® Windows Server® 2008 Enterprise	Data Base Server Ley 404 Histórico
Policia14	VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	File Server
Policia15	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Sistema De Alerta Temprano
Policia16	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	File Server 'SARP"
Policia17	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Data Base Server
Policia18	VMware Virtual Platform	Microsoft® Windows Server® 2008 Enterprise	File Server
Policia19	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	File Server: Asuntos Organizacionales. (Órdenes y Reglamentos)
Policia20	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Sistema de Alerta Temprano
Policia21	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Sistema de Alerta Temprano
Policia22	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	App Server Sistema Asistencia
Policia23	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	Data Base Server
Policia24	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	Data Base Server "Violencia Domestica"
Policia25	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	Data Base Server
Policia26	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	

Nombre	Modelo	Sistema Operativo	Descripción
Policia27	VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	App Server Sistema Violencia Domestica
Policia28	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	App Server Sistema Asistencia
Policia29	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	
Policia30	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Sistema De Monitoreo EMC
Policia31	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Sistema De Inventario
Policia32	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Sistema De Monitoreo Opmanager
Policia33	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	App Server Sistema De Asistencia
Policia34	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	App & Data Base Server Sistema De Asistencia
Policia35	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Enterprise	File Server
Policia36	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Data Base Server
Policia37	VMware Virtual Platform	Microsoft® Windows Server® 2008 Enterprise	Data Base Server
Policia38	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	File Server División De Presupuesto
Policia39	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	File Server Vehículo Hurtado
Policia40	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	Data Base Corrección & DTOP
Policia41	VMware Virtual Platform	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	Data Base Server Rh
Policia42	VMware Virtual Platform	Microsoft Windows Xp Professional	Nomina Histórica
Policia43	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Data Base & File Server, Prifas
Policia44	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Data Base & File Server, CIW

Tabla de Servidores en orden de apagado

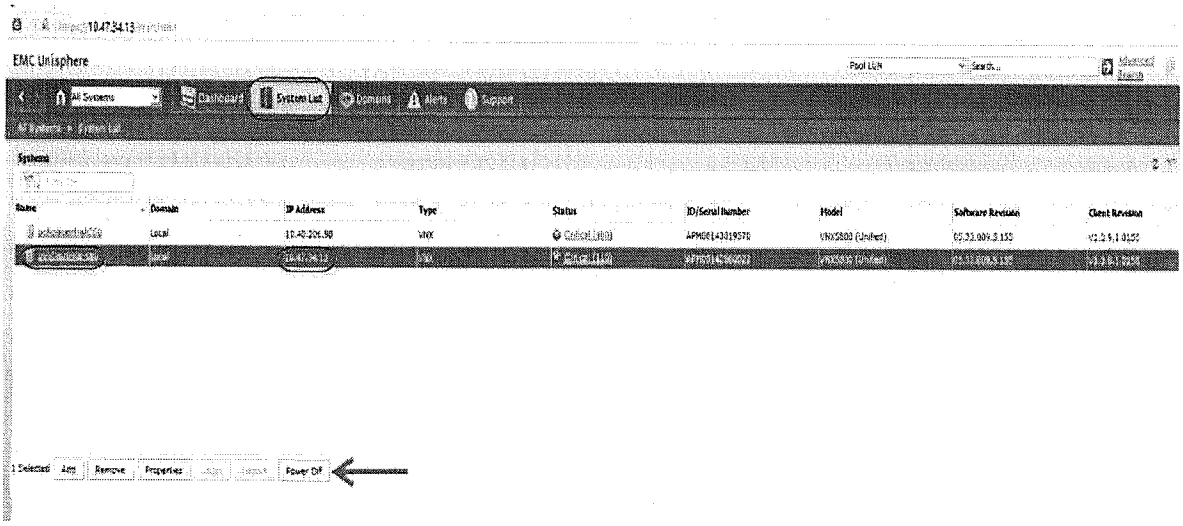
Falla total del Sistema Eléctrico Público y del Sistema de Planta de Emergencia

Nombre	Modelo	Sistema Operativo	Descripción
Policia45	IBM System x3690 X5	Microsoft Windows Server 2008 R2 Enterprise	App &Data Base Server, Sistema LPH
Policia46	IBM System x3690 X5	Microsoft Windows Server 2008 R2 Enterprise	App &Data Base Server, Sistema LPH
Policia47	VMWare Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Exchange Syncronization Server

Nombre	Modelo	Sistema Operativo	Descripción
Policia48	IBM System x3850 X5	Microsoft Windows Server 2012 R2 Standard	Exchange Server Hybrid Office 365
Policia49	IBM System x3850 X5	Microsoft Windows Server 2012 R2 Standard	Networker Server
Policia50	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	DHCP Voice Server
Policia51	PowerEdge R910	Microsoft Windows Server 2012 R2 Standard	DHCP Voice Server
Policia52	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	Data Base Server, Sistema de Armas (Ley 404)
Policia53	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	DHCP Data Server
Policia54	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Data Base Server (343-2020)
Policia55	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Web Server Sistema de Armas (Ley 404) & CrimeMapping
Policia56	VMware Virtual Platform	Microsoft® Windows Server® 2008 Standard	Print Server
Policia57	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Data Base Server Sistema CrimeMapping
Policia58	PowerEdge R910	Microsoft Windows Server 2008 R2 Standard	Web Server CrimeMapping
Policia59	PowerEdge R910	Microsoft Windows Server 2008 R2 Standard	App, Data & Storage Server Base, Sistema Digitalización
Policia60	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	System Center Endpoint Protection
Policia61	PowerEdge R710	Microsoft Windows Server 2012 R2 Standard	Host VMware
Policia62	VMware Virtual Platform	Microsoft Windows Server 2012 R2 Standard	Print Server
Policia63	IBM System x -[7871AC1]-	Microsoft Windows Server 2008 R2 Standard	Sistema de Backups
Policia64	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Domain Controller
Policia65	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Domain Controller
Policia66	VMware Virtual Platform	Microsoft Windows Server 2008 R2 Standard	Sistema de Administración Infraestructura Virtual

c. Procedimientos para desactivar (Shutdown) el Sistema de Almacenamiento "VNX 5800 y DD2500" San Juan y Ponce.

A continuación, se muestra el proceso para desactivar el sistema:



B. Acciones después de la Contingencia

1. Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para restablecer los equipos activos y servicios.
2. Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina. Tomando en cuenta el siguiente orden:

    a. Validar el correcto funcionamiento de los equipos activos y servicios.
    b. Identificar los posibles daños de los equipos activos.
    c. Notificar a los usuarios afectados el restablecimiento de los servicios y su condición.
    d. Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las áreas involucradas.

XII. PLAN DE CONTINUIDAD PARA CUIDAR LA INTEGRIDAD DEL PERSONAL

A. Acciones antes de la contingencia

1. Programar 2 simulacros al año.
2. Programar dos fumigaciones anuales, en periodos vacacionales.
3. Conocer el manejo de los extintores.
4. Contar con botiquines de primeros auxilios en áreas estratégicas.
5. Contar con capacitación de primeros auxilios.
6. Implementar alarmas de emergencia en lugares estratégicos dentro del Cuartel General del NPPR.
7. Establecer puntos de reunión dentro y fuera del Cuartel General del NPPR.
8. Difundir las rutas de evacuación, así como los sitios de localización de alarmas, extintores.

9. Establecer procedimientos de desalojo.
10. Capacitación permanente y actualizada a los comités de Seguridad del Centro de Cómputo.
11. Contar con un directorio del personal.

B. Acciones durante la contingencia

1. Accionar las alarmas de emergencia.
2. Dirigir a los usuarios en el desalojo e información de salidas de emergencia.
3. Priorizar la evacuación.
4. Llamar al 911.

C. Acciones después de la contingencia

1. Brindar los primeros auxilios a las personas que lo requieran.
2. Realizar un recuento de los daños causados.
3. Realizar un informe con los hallazgos y emitir a la Dirección.
4. Tomar acciones de acuerdo con el informe emitido.
5. Retroalimentar los planes de contingencia con lo aprendido en la última contingencia.

D. Documentos Necesarios Previos a las Contingencias

1. Contar con una copia del inventario del mobiliario y equipo existente en el área.
2. Contar con un listado de configuraciones del equipo de cómputo y telecomunicaciones que reside en el área.
3. Contar con documentación al día de contratos de mantenimiento de infraestructura.

XIII. PLAN PARA CONTINUAR OPERACIONES LUGAR ALTERNO

E. Acciones necesarias para continuar operaciones en Comandancia de Ponce cuando el Cuartel General no esté operando

1. Brindar un tiempo de gracia (depende de la magnitud de la contingencia) para restablecer los equipos activos y servicios en lugar alterno (Comandancia de Ponce).
2. Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina. Tomando en cuenta el siguiente orden:
   a. Validar el correcto funcionamiento de los equipos activos y servicios.
   b. Identificar los posibles daños de los equipos activos.
   c. Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las áreas involucradas.

d. Notificar a los usuarios afectados el restablecimiento de los servicios, movimiento de los mismo y su condición en el lugar alterno designado.

Este plan está sujeto revisión anual o según la necesidad del Negociado de La Policía.