GOBIERNO DE PUERTO RICO

Negociado de la Policía de Puerto Rico

MANUAL PARA LA ADMINISTRACIÓN DE LOS SISTEMAS COMPUTADORIZADOS

2018

ÍNDICE

I. INTRODUCCIÓN

Con la creación del Manual para la Administración de los Sistemas Computadorizados, se busca establecer en el Negociado de la Policía de Puerto Rico (NPPR) una cultura de calidad en el uso responsable de los sistemas computadorizados. La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas, procedimientos y estándares que cubran las necesidades de la División de Tecnologías del NPPR en materia de seguridad.

El manual tiene como objetivo mejorar el desempeño, en términos de eficiencia y eficacia de la Agencia, mediante la regulación y estandarización de la infraestructura de tecnología considerando la secuencia de actividades orientadas a las prácticas generalmente aceptadas. Además, comprende todos los aspectos de administración y operación que rigen las funciones y/o actividades de la Agencia, así como la identificación de áreas de oportunidad para mejorar la calidad, el desempeño operativo y la satisfacción de los usuarios.

Asimismo, el estructurar los procesos y procedimientos relacionados con la tecnología, desde su planteamiento estratégico hasta su organización operativa, permite crear esquemas óptimos para brindar un servicio de excelencia, y así poder evaluar indicadores administrativos, operacionales e investigativos.

Este manual está desarrollado 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) y la Orden General Capítulo 400, Sección 403, titulada: Normas para el Uso de los Sistemas Computadorizados (OG 403).

II. Desarrollo General

A. APLICACIÓN

El Manual para la Administración de los Sistemas Computadorizados tiene por objeto establecer medidas y estándares técnicos de administración y organización de las tecnologías de información de todo el personal del NPPR, en el uso de los servicios informáticos proporcionados por la División de Tecnologías (DT), nombre asignado al área de sistemas de información, mediante la OG 403, en cuanto a las prácticas generalmente aceptadas en las tecnologías de la informática (TI) y al cumplimiento de los objetivos institucionales.

Este documento se convierte en una herramienta de difusión sobre los procesos y procedimientos, en términos de la administración de los sistemas de información y TI del NPPR. Esto para facilitar una mayor integridad, confidencialidad y confiabilidad de la información generada por la DT al personal, al manejo de los datos y al uso de los bienes informáticos tanto de hardware como de software, y por consiguiente minimizar los riesgos en el uso de las TI. Además, las políticas y procedimientos relacionadas al uso de las TI en la Agencia tendrán una revisión periódica (anual) para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones que brindan los usuarios, el personal de apoyo técnico y administrativo. De ser necesario o de surgir alguna tecnología o estándar que amerite adelantar la revisión, se comenzara el proceso mediante consulta y aprobación del Director del Negociado de Tecnologías y Comunicaciones (CIO).

III. SEGURIDAD INSTITUCIONAL

Todo empleado y/o personal del NPPR, antes de manejar equipos electrónicos computadorizados y hacer uso de servicios informáticos, debe aceptar las condiciones de confidencialidad, condiciones de uso adecuado de los bienes y servicios informáticos, así como cumplir y respetar las directrices impartidas por el Negociado de Tecnologías y Comunicaciones (NTC).

Los equipos computadorizados, las redes de comunicaciones de datos y computadoras (incluyendo las redes inalámbricas), así como los sistemas de información implementados en el NPPR, son recursos esenciales para lograr el trabajo diario en términos operacionales, administrativos e investigativos de la Agencia. Por ende, la otorgación de acceso compartido a dichos recursos al igual que a las fuentes de información local y/o nacional, se deberán utilizar y manejar responsablemente para asegurar su integridad, seguridad y disponibilidad para actividades apropiadas de carácter operacional, administrativo e investigativo. Se requiere que los empleados y/o personal del NPPR que utilicen estos recursos de forma eficiente, eficaz y responsable, de manera que no se afecten los servicios apoyados por la infraestructura tecnológica en términos de disponibilidad y seguridad de datos e información que se procesen y generen en los sistemas de información del NPPR.

Todo empleado del NPPR o contratista tendrá la obligación de cumplir con las disposiciones de este Manual y de informar a su supervisor inmediato cualquier violación a estas normas. Aquel miembro del NPPR que incumpla con cualquier disposición de este Manual, estará sujeto a sanciones disciplinarias y/o criminales, según corresponda. El NPPR referirá a la Superintendencia Auxiliar en Responsabilidad Profesional (SARP) para su investigación de forma inmediata cualquier violación de alguna ley o política de la Agencia. Asimismo, el NTC tomará todas las medidas necesarias y/o preventivas para restringir o limitar el acceso a los sistemas de información y tecnología con el fin de proteger la infraestructura y buen funcionamiento de la tecnología.

IV. SEGURIDAD FÍSICA Y AMBIENTAL

Para el acceso al Centro de Cómputos del NPPR se notificará a la DT para la autorización correspondiente.

A. CONTROLES DE ACCESO FÍSICO

1. Cualquier persona que tenga acceso al Centro de Cómputos, registrará al momento de su entrada, cualquier equipo tecnológico, medios de almacenamiento y herramientas, que no sean propiedad del NPPR, en el área de recepción del Centro de Cómputos.
2. Las computadoras personales y computadoras portátiles, o cualquier activo de tecnología de información, podrá ser retirado de las instalaciones del NPPR únicamente con la autorización de salida del Área de Inventarios, anexando el comunicado de autorización del equipo debidamente firmado por el Director de o el Encargado de la Propiedad de la DT.

B. SEGURIDAD EN ÁREAS DE TRABAJO

El Centro de Cómputos es un área restringida, por lo que sólo el personal autorizado por la DT puede acceder.

C. MANTENIMIENTO DE EQUIPOS

1. Únicamente el personal autorizado por la DT podrá llevar a cabo los servicios y reparaciones de los equipos tecnológicos.
2. La DT no se hace responsable de información guardada en los equipos o computadoras cuando se envíen a reparación. Los usuarios se asegurarán de respaldar en copias de respaldo o "backups" la información que consideren relevante cuando su computadora sea enviada a reparación y borrarán aquella información sensible que se encuentre en el equipo, evitando así, la pérdida de información, derivada del proceso de reparación.

V. ADMINISTRACIÓN DE OPERACIONES EN EL CENTRO DE CÓMPUTOS

A. OPERACIONES

La DT, desarrollará las políticas y procedimientos administrativos para regular, controlar y permitir el acceso de visitantes o funcionarios no autorizados a las instalaciones del Centro de Cómputo restringidas.

1. Cuando un funcionario no autorizado requiere la necesidad de ingresar al Centro de Cómputos, solicitará el acceso mediante comunicado interno debidamente firmado y autorizado por el Director de la DT o el Director del NTC. Cuando se trate de un visitante se solicitará autorización al Director de la DT o del NTC, con tiempo razonable. Dicha solicitud de visita será consultada con el Director del NTC, y especificará el tipo de actividad a realizar. Durante la visita, siempre contará con la presencia de un funcionario de la DT.
2. El Director de la DT tendrá un registro escrito de todas las visitas autorizadas y realizadas al Centro de Cómputos.
3. Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputos, se le dará aviso con anticipación a los usuarios de la interrupción del servicio.
4. El Centro de Cómputos contará con los equipos de protección contra incendios, inundaciones, y sistema eléctrico de respaldo (UPS). El Director del NTC, así como el Director de la DT velarán por el cumplimiento de esta disposición.

B. USO DE MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN CLASIFICADA

1. La DT conservará los registros y la información que se encuentra activa, así como aquella información que ha sido clasificada como confidencial.
2. Las actividades que realicen los usuarios en la infraestructura tecnológica del NPPR estarán registradas y serán objeto de auditoría.

C. ADQUISICIÓN DE SOFTWARE

1. La DT tendrá el control y manejo de las licencias, en cualquier medio, de los softwares adquiridos por el NPPR.
2. El Grupo de Apoyo Técnico de la DT velará por el buen uso de los equipos de cómputo y del cumplimiento de las políticas de seguridad. A su vez, ofrecerá mantenimiento preventivo a los equipos computadorizados de la Agencia.
3. El Grupo de Apoyo Técnico mantendrá un inventario de equipos físicos y programas instalados. Además, están autorizados para borrar o instalar software adquiridos y legalmente licenciados por la Agencia. Cualquier otra petición de software deberá ser tramitada a través de la DT, utilizando el sistema para llamadas de servicios del área de Help Desk.

D. LICENCIAMIENTO DE SOFTWARE

1. Para el Control de Licenciamiento de Software, el NPPR cuenta con un contrato con vigencia anual, a través de la Oficina de Gerencia y Presupuesto (OGP). Además, como política de seguridad, se tiene establecido la prohibición de instalar software no autorizados y sin licencia.
2. La DT realizará un inventario de los softwares instalados en cada uno de los equipos computadorizados de la Agencia, anualmente.

E. IDENTIFICACIÓN DEL INCIDENTE

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del NPPR será reportado a la DT.

F. ADMINISTRACIÓN DE LA RED

Los usuarios del NPPR no establecerán redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red, sin la autorización de la DT.

G. SEGURIDAD PARA LA RED DE COMUNICACIONES DE DATOS

Será considerado como un ataque a la seguridad informática, cualquier actividad no autorizada por la DT, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red del NPPR, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

H. CONTROLES CONTRA VIRUS O SOFTWARE MALICIOSO

1. El NPPR utiliza un software de antivirus autorizado y licenciado que diagnostica actividades de virus en los equipos computadorizados de la Agencia. El software de antivirus está configurado para que se actualice automáticamente.
2. Ningún usuario o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la DT.

I. CONTROLES PARA LA GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO ("BACKUPS")

En el procedimiento de generación y restauración de copias de respaldo para salvaguardar los datos e información crítica sobre las transacciones diarias, procesos y procedimientos significativos del NPPR, se considerarán como mínimo los siguientes aspectos:

1. Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o Backups periódicamente en los sistemas tecnológicos del NPPR.
2. El Área de Operaciones del Centro de Cómputos es responsable directo de la generación de los "Backups" o copias de respaldo de los sistemas tecnológicos del NPPR.
3. Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las

copias de respaldo, debidamente marcadas. Almacenamiento interno de las copias de respaldo.

4. Las copias de seguridad o "Backups" es un proceso automático que se realiza diariamente. Un Operador del Centro de Cómputos de la DT, revisará diariamente el cumplimiento de este procedimiento revisando los registros del proceso. En el caso de falla, procederá a realizar manualmente el resguardo.

J. PLAN DE CONTINGENCIA ANTE DESASTRE

Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios operacionales, administrativos e investigativos, la DT tendrá la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastres. Dicho plan empleará los siguientes principios:

1. Disponibilidad de una infraestructura tecnológica que soporte los sistemas tecnológicos, comunicaciones e información, necesarias para soportar las operaciones definidas como misión crítica del NPPR en los tiempos esperados y acordados.
2. Tener en existencia equipos informáticos de respaldo en una localidad alterna o en la nube, necesarios para la puesta en marcha la recuperación de los servicios tecnológicos.
3. Existencia de documentación de los procedimientos manuales a seguir por las distintas áreas que utilicen equipo computadorizado durante el periodo de la contingencia. El NTC tiene la responsabilidad de adiestrar el personal que participa en estos procesos y/o procedimientos.
4. Existencia de documentación de los procesos y/o procedimientos detallados para restaurar equipos, aplicativos, sistemas operativos, bases de datos, y archivos de información, entre otros.
5. Existencia de documentación de pruebas periódicas de la implementación del plan de recuperación ante desastre para verificar tiempos de respuesta,

capitalizando los resultados de las pruebas para la implementación efectiva del plan.

6. Actualización periódica del plan de recuperación ante desastre, de acuerdo con los cambios en la infraestructura tecnológica (hardware, software y comunicaciones), para reflejar permanentemente la realidad operativa y tecnológica del NPPR.
7. Disponibilidad de copias de respaldo en un lugar alterno del Cuartel General del NPPR para restablecer las operaciones de misión crítica definidas.

K. INTERNET

1. Todos los accesos al Internet tienen que ser realizados a través de los canales de acceso provistos por el NPPR. En caso de necesitar una conexión a Internet alterna o especial, ésta debe ser solicitada mediante comunicación escrita acompañada de la PPR-403.1 titulado "Solicitud de Acceso" (PPR-403.1) y ser aprobada por la DT.
2. Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:
   a. Serán sujetos de monitoreo de las actividades que realizan en Internet.
   b. Está terminantemente prohibido acceder a páginas no autorizadas, y la transmisión de archivos confidenciales no autorizados.
   c. Se prohíbe descargar software sin la autorización de la DT.
   d. La utilización de Internet es para el desempeño de sus funciones y no para propósitos personales.

L. ADMINISTRACIÓN DE PRIVILEGIOS

Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a la DT a través de la PPR-403.1.

M. ADMINISTRACIÓN Y USO DE CONTRASEÑAS

1. La asignación de contraseñas será realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá solicitar a través de una llamada de servicio al Help Desk de la DT para que se le proporcione una nueva contraseña.
3. Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.

N. CONTROLES PARA OTORGAR, MODIFICAR Y RETIRAR ACCESOS A USUARIOS

1. Todo usuario quedará registrado en la Base de Datos de Usuarios y Roles. La creación de un nuevo usuario y/o solicitud para la asignación de otros roles dentro del sistema del NPPR, deberá de venir acompañado del formulario PPR-403.1 debidamente firmado por el Director o Supervisor de Área y con el visto bueno del Director de la DT o el Director del NTC, de lo contrario no se tramitará dicha solicitud.
2. La DT, entiéndase, su Director o su representante en caso de ausencia, será la responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios.

O. CONTROL DE ACCESOS REMOTO

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro (VPN) autorizado por el dueño de la información y de la DT.

VI. CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

La DT tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de equipo computadorizado, así como de bancos de datos de información automatizada en general.

El cumplimiento de las políticas de seguridad de la información es de carácter obligatorio para todos los niveles en la Agencia: entiéndase los usuarios que pertenecen al sistema de rango, personal del sistema clasificado, contratistas independientes, reservistas, proveedores de servicios y consultores. Cada individuo debe entender su rol y asumir su responsabilidad respecto al cumplimiento de las políticas de seguridad acorde con sus funciones dentro del NPPR.

Cualquier incumplimiento de estas Políticas que comprometa la integridad, confidencialidad y disponibilidad de la información, resultará en una investigación administrativa de aplicar, terminación de contratos de trabajo y acciones legales que sean pertinentes.

A. DERECHOS DE PROPIEDAD INTELECTUAL

Los sistemas desarrollados por personal interno o externo que contrate la DT son propiedad intelectual del NPPR. Los mismos se regirán por lo establecido en el Reglamento para la Protección de los Derechos de Autor y Propiedad Intelectual del NPPR.

B. CLÁUSULAS DE CUMPLIMIENTO

1. La DT supervisará el cumplimiento del Manual para la Administración de los Sistemas Computadorizados.
2. La DT podrá desarrollar e implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado, será reportado conforme a lo indicado en la política de seguridad de personal.
3. Los directores de divisiones y responsables de los procesos establecidos en la DT deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas, así como cualquier otro requerimiento de seguridad.

C. VIOLACIONES DE SEGURIDAD INFORMÁTICA

1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática, a menos que se autorice por la DT.
2. Está terminantemente prohibido que los usuarios y/o funcionarios de la DT pretendan o intenten hacer pruebas sobre fallas o vulnerabilidades en la seguridad de los sistemas de información, a menos que estas pruebas sean controladas y aprobadas por la DT en consulta con el CIO.
3. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar, afectar el desempeño y acceso a los equipos computadorizados, redes o información del NPPR.

D. EQUIPOS EN EL ÁREA ADMINISTRATIVA

1. La DT, será quien valide el cumplimiento de las condiciones técnicas de los equipos tecnológicos, tales como, servidores, desktops, laptop, dispositivos móviles y periféricos adquiridos por la Agencia.
2. La DT, tendrá bajo su resguardo las licencias de software, medios originales, licencias electrónicas, manuales originales, así como un medio físico de respaldo para su instalación. Además, llevará el control de software instalado en los equipos tecnológicos (servidores, desktops, laptop, dispositivos móviles y periféricos) al momento de la recepción de los mismos.
3. Los requerimientos de equipos tecnológicos se llevarán a cabo mediante la solicitud y justificación por escrito, firmada por el director del área que lo solicita, los cuales serán evaluados por la DT y el CIO con el fin de autorizar y solicitar el presupuesto correspondiente para fines de compras.
4. La DT, se encarga de tramitar las asignaciones, reasignaciones y bajas de equipos informáticos computadorizados de escritorio, portátiles y periféricos ante la Sección Financiera. Dicha sección, se encarga del Inventario de Activos

para su ejecución, en base a las solicitudes realizadas al respecto y las revisiones sobre la vida útil de los mismos.

5. El grupo de apoyo técnico de la DT, elaborará y registrará en cada asignación o movimiento de equipos computadorizados, (desktop, laptop, impresoras y otros), a través de una llamada de servicio indicando adquisición, reparación, actualización, mantenimiento o cambio de materiales y equipos, el cual se realizará llamando al área de Help Desk de la División de Tecnología.

6. La DT elaborará un pase de salida cuando algún bien tecnológico (desktop, laptop, impresoras y otros) requiera ser trasladado fuera de las instalaciones del NPPR por motivo de garantía, reparación o evento.

7. Si algún equipo tecnológico (desktop, laptop, impresoras y otros) es trasladado por el usuario a oficinas distintas al lugar asignado, ya sea a oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el equipo y el pase de salida quedará a consideración de la DT para su autorización y visto bueno.

8. Las diferentes Áreas del NPPR serán encargadas de proporcionar a la DT, la relación de bienes y equipos que entrarán al proceso de decomiso, según corresponda. La DT realizará la evaluación técnica del equipo y definirá la reasignación o decomiso definitivo del bien, y será informada la División de Propiedad para control de inventarios de activos por medio del procedimiento establecido.

9. Se prohíbe la baja o decomiso de equipo tecnológico que no cuente con la evaluación técnica por parte del personal de la DT.

10. Queda prohibido instalar software no autorizado o que no cuente con licencia, la DT será quien realice las instalaciones de acuerdo con los estándares del NPPR.

11. El Software autorizado para todos los equipos computadorizados del cual la DT cuenta con licencia de uso son los siguientes:

    a. Sistemas Operativos para desktop y laptop.

b. Sistema Operativo para servidores.
c. Suite de software para correo electrónico y productividad.
d. Software para la creación y administración de bases de datos.

E. ROLES DE LA DIVISIÓN DE TECNOLOGÍA

Funciones específicas para todo el personal integrante de la DT:

1. Administrar y evaluar los requerimientos de información de las distintas áreas del NPPR.
2. Coordinar con el equipo de apoyo de la DT en la definición, factibilidad, especificación y validación de requerimientos.
3. Vigilar la correcta aplicación de los estándares y metodologías de desarrollo de sistemas de información, así como sugerir las mejoras que sean necesarias.
4. Coordinar con los usuarios de las distintas dependencias para la definición de requerimientos funcionales y no funcionales de los sistemas de información.
5. Revisar, aprobar y mantener actualizados los manuales, de operación y de usuario, concerniente a los sistemas de información y tecnológicos implementados en el NPPR.
6. Elaborar reportes de avance y estrategias de ejecución de los proyectos de desarrollo de sistemas de información.
7. Desarrollar e implementar los sistemas de información que requieran las dependencias, de acuerdo a las prioridades establecidas en el plan de cumplimiento de la Reforma Sostenible del NPPR.
8. Efectuar el mantenimiento y actualización de los sistemas de información, analizando los problemas o planteamientos de modificación, garantizando su correcta sincronización.
9. Participar en los procesos de adquisición y pruebas de las soluciones informáticas de terceros. Asimismo, supervisar las actividades realizadas por terceros en el desarrollo e implementación de soluciones informáticas.

10. Apoyar en la capacitación al usuario final y al personal designado de la Sección Apoyo Técnico, en el adecuado uso de los sistemas de información, así como proporcionar material de soporte y los medios necesarios para tales fines.
11. Administrar en forma eficiente los recursos asignados a la división, así como el Centro de Cómputos, velando por la seguridad de accesos y operatividad, protegiendo la información de ingreso, salida y almacenamiento.
12. Participar en la elaboración de la propuesta del Plan de Actividades de la división, en los planes de contingencia y en la implementación de acciones que minimicen el riesgo de las TI.
13. Verificar que el personal de la DT atienda oportuna y eficientemente los requerimientos de las dependencias, supervisando el cumplimiento de las metodologías, estándares y/o técnicas implementadas.
14. Cumplir y hacer cumplir las medidas correctivas recomendadas por los entes de vigilancia y control, tanto externos como internos.
15. Ejecutar los planes de respaldo y las recuperaciones de información que se requieran para garantizar la continuidad operativa de las actividades.
16. Atender asuntos relativos al servicio de Apoyo Técnico de primer nivel para la solución de problemas referidos sobre hardware, software, comunicaciones y servicios tecnológicos, efectuados por el personal de la división y por todas las dependencias del NPPR.
17. Participar en los procesos de atención de los problemas y reclamos.
18. Atender consultas técnicas, operativas y funcionales a los usuarios, incentivándolos en el mejor uso y operación de las TI.
19. Representar la Agencia ante los organismos competentes gubernamentales y no gubernamentales.
20. Ejecutar, instalar y configurar los equipos de computadoras y periféricos en todas las dependencias del NPPR, cumpliendo con los procedimientos y estándares aprobados.
21. Instalar y diagnosticar los daños del cableado estructurado de la red local (LAN) en todas las dependencias del NPPR.

22. Coordinar, analizar las incidencias y magnitudes de un desastre, determinando prioridades de atención, así como disminuir el nivel de riesgos en la operación.
23. Determinar y gestionar de inmediato las actividades a realizar para generar una solución y hacer funcionar en el menor tiempo posible todos los sistemas de información colapsados ante un desastre.

F. ADMINISTRACIÓN DE LA RED DE COMUNICACIONES DE DATOS Y COMPUTADORAS

El Administrador de la red de Comunicaciones de Datos y Computadoras, adscrito a la DT, será responsable de los recursos constituidos por equipos (router, bridges, switch, etc.) de medios de comunicación de datos (Fast Ethernet, Gigabyte Ethernet, E1, T1, E3, STM-1, etc.). Además, velará por las condiciones óptimas de las redes internas que se conectan a otras redes (corporativas, Internet), lo que hace que se vuelvan más complejas y robustas. Estará a cargo de las siguientes cinco (5) áreas:

1. Administración del Desempeño (Performance Management): Se encarga de monitorear y medir varios aspectos de rendimiento, funcionamiento y utilización de la red, con el fin de mantener en niveles aceptables los servicios que se encuentran disponibles, así como rastrear todos los efectos en su operación.
2. Administración de la configuración (Configuration Management): Administra y evalúa los aspectos de configuración de los dispositivos de la red, como los archivos de configuración de dichos dispositivos, y administración del software; así como el almacenamiento en un lugar que sea accesible por el personal autorizado.
3. Administración de la Contabilidad (Accounting Management): Gestiona y genera la información que permite describir el uso de los recursos que conforman la red. El primer paso es medir la utilización de todos los recursos para luego realizar un análisis de que proporcione el patrón de comportamiento actual de uso de la red, de aquí también se puede obtener información que ayude a planear un crecimiento o actualización de cada elemento que forma parte de la red, así como determinar si dicho uso es justo y adecuado.

4. Administración de Fallas (Fault Management): Detecta, registra, aísla, notifica y corrige fallas en aquellos equipos que son parte de la red que presenten algún problema que afecte su buen funcionamiento. Es importante aclarar que cualquier problema que se presente se verá reflejado como una degradación en los servicios que ofrece la red. El proceso inicia desde la detección y determinación de síntomas, hasta el registro del problema y su solución.
5. Administración de la Seguridad (Security Management): Controla el acceso a los recursos de la red de acuerdo a las políticas establecidas, con el fin de evitar algún abuso y la pérdida de la confidencialidad; entre las funciones está identificar los recursos sensibles y críticos de la red, y monitorear los accesos.

Este manual entrará en vigor el 26 de Junio de 2018.

Henry Escalera Rivera
Comisionado