MUSEO NACIONAL DE COSTA RICA

Dirección General

Unidad de Informática

Plan de Contingencias de Tecnologías de Información del Museo Nacional de Costa Rica

Elaborado por:

Unidad de Informática

Diciembre, 2019

APROBADO POR JUNTA ADMINISTRATIVA DEL MNCR

EN EL ACUERDO A-19-1346, DE LA SESIÓN NÚMERO: 1346, DEL 12 DE DICIEMBRE DEL 2019

TABLA DE CONTENIDO

INTRODUCCIÓN

Un plan de contingencia es un conjunto de procedimientos alternativos a la operatividad normal de cada institución, su finalidad es permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo como resultado de algún incidente tanto interno como ajeno a la institución.

Todas las instituciones deberían contar con un plan de contingencia actualizado, valiosa herramienta en general basada en un análisis de riesgo, la cual permitirá ejecutar un conjunto de procedimientos y acciones básicas de respuesta que se debería tomar para afrontar de manera oportuna, adecuada y efectiva, ante la eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir tanto en las instalaciones como fuera de ella.

Es por eso que se hace imperativo la definición de una serie de normas claras que regulen las acciones que se deben realizar en caso de que uno de los riesgos se materialice, garantizando niveles adecuados de seguridad y minimizando las vulnerabilidades inherentes a la tecnología.

Los riesgos los puedes eliminar, transferir, mitigar o aceptar. Ello dependerá de varios factores tales como la probabilidad de ocurrencia o impacto del riesgo.

OBJETIVO

Mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que se encuentran a disposición del Museo Nacional de Costa Rica.

ALCANCE

Las presentes normas son de aplicación en la Unidad de Informática y los usuarios involucrados con el uso de equipo de cómputo en el Museo Nacional de Costa Rica.

PLANIFICACIÓN Y ORGANIZACIÓN

UNIDAD DE INFORMÁTICA

La Unidad de Informática es la encargada de velar en el Museo Nacional en todo lo que respecta a tecnologías de información, encargada del buen funcionamiento de los Equipos de Cómputo, Sistemas y Telecomunicaciones.

Conformado por cinco funcionarios los cuales son los encargados de atender todas las sedes del Museo Nacional de Costa Rica.

OBJETIVO GENERAL:

Identificar las actividades y proyectos de trabajo de la Unidad de Informática, o en los que esta tiene que dar apoyo o asesoría, y así tener una idea clara de las labores a desarrollar, así como de las metas que se necesitan alcanzar estableciendo de manera clara las funciones de desarrollo y apoyo de las tecnologías de información en la Institución.

OBJETIVOS ESPECÍFICOS

a) Gestionar la infraestructura tecnológica que soporte eficientemente los servicios de tecnologías de información y comunicación.

b) Modernizar los sistemas de administración de información de colecciones de patrimonio natural y cultural (bases de datos) existentes en la institución.

c) Modernizar los sistemas de información fundamentales para hacer eficientes los servicios administrativos que demanda el funcionamiento del Museo Nacional de Costa Rica.

d) Mantener actualizados los equipos informáticos necesarios para el manejo de colecciones, la investigación del patrimonio, la proyección de información al público y la administración de recursos en el Museo Nacional.

e) Mantener actualizados los sistemas de comunicación entre las diferentes sedes del Museo Nacional de Costa Rica.

f) Asegurar que los servicios informáticos brindados sean oportunos y que satisfagan las necesidades de los usuarios.

g) Mejorar la administración de los equipos y software para aprovechar de mejor modo las tecnologías de información en las labores de trabajo en el Museo Nacional de Costa Rica.

h) Fortalecimiento del control interno respecto a tecnología de información.

IDENTIFICACIÓN DE RIESGOS

Lo siguiente es un recuento de los posibles riesgos a los cuales están expuestos los equipos de tecnología de información y la información generada, procesada y almacenada en estos equipos:

INCENDIO

La mayoría de los departamentos no están preparados para combatir el fuego, a pesar de que en todas las oficinas se cuenta con extintores con la carga actualizada. Es por ello que se debe considerar que todos los activos se pueden ver expuestos a este riesgo.

FALTA DE FLUIDO ELÉCTRICO

Todos los equipos de tecnologías de información cuentan con una UPS, la cual brindará un tiempo reducido para guardar los documentos y apagar los equipos de manera adecuada, en caso de un problema grave con el fluido eléctrico. Sin embargo, estas UPS no permitirán el funcionamiento prolongado de los equipos de tecnologías de información.

ROBO O FRAUDE

A pesar de contar con cámaras de video vigilancia en los pasillos y salas de exhibición, la Institución no está exenta del riesgo de robo o fraude, a nivel de información física o digital (documentos impresos, CD, DVD, llaves USB, entre otros).

VANDALISMO Y/O TERRORISMO

Es un riesgo que sufre la institución al tener información de interés nacional en diversas áreas de exploración, del patrimonio cultural y natural. Personas mal intencionadas pueden querer alterar esta información para su beneficio personal o lucrar con estos datos.

ATAQUE DE VIRUS

Es un riesgo con el cual tienen que convivir todas las instituciones.

DESASTRE NATURAL

Es casi imposible prever un desastre natural llámese terremoto, tornado o inundación por lluvias. Lo que se debe hacer es capacitar al personal de la Institución e indicar al personal de seguridad cuáles equipos debe salvar, siempre y cuando no pongan en peligro la vida humana.

DAÑOS PARCIALES DEL EQUIPO

Los daños parciales a componentes o aparatos individuales del equipo, son causados por agentes externos, como lo son la consecuencia de errores de manejo, trato inadecuado del equipo, el efecto del agua, polvo o suciedad. Este tipo de daños por lo general son poco frecuentes pero el costo de estos cuando se presentan es elevado; por lo tanto, debe ser un riesgo tomado en cuenta.

PÉRDIDA DE INFORMACIÓN DE LAS BASES DE DATOS DE COLECCIONES

El personal a cargo de introducir la información o hacer cambios en las bases de datos de colecciones debe conocer el procedimiento y estar debidamente autorizado para hacer esta labor. El acceso a las bases de datos es un riesgo potencial que debe ser tomado en consideración. En la actualidad cada Departamento cuenta con acceso a las bases de datos de colecciones.

FALLAS EN LOS RESPALDOS DE INFORMACIÓN

La actualización e incorporación de nueva información en las bases de datos debe respaldarse constantemente. Uno de los respaldos debe ser almacenado en una ubicación diferente al centro de datos y designar el responsable para el cumplimiento de esta labor.

ANALISIS DE RIESGOS

A continuación de detalla el análisis de Probabilidad x Impacto para los riegos identificados en el apartado anterior.

Suceso	Impacto	Probabilidad
Incendio	ALTA	ALTA
Falta de Fluido Eléctrico	MEDIA	ALTA
Robo o Fraude	ALTA	BAJA
Vandalismo y/o Terrorismo	ALTA	MEDIA
Ataque de Virus	BAJA	ALTA
Desastre Natural	ALTA	BAJA
Daños parciales de Equipos	MEDIA	BAJA
Pérdida de información de las bases de datos de colecciones	BAJA	MEDIA
Omisión de hacer respaldos de la información de colecciones	ALTA	MEDIA

Se tienen en cuenta dos factores:

- Los que afectan a la seguridad del edificio.
- Los que afectan la integridad de los datos.

Los que afectan a la seguridad del edificio:

- **Inundación:** ocasionaría pérdidas totales o parciales, por lo tanto, actividades interrumpidas hasta solucionar el problema.
- **Incendio:** ocasionaría pérdidas totales o parciales.
- **Corte de energía eléctrica:** En caso del Museo Nacional de Costa Rica, no existe una planta o generador que proporcione la energía eléctrica para todo el edificio, generaría discontinuidad en el trabajo en oficinas. También generaría caída total de los sistemas del Museo, caída total de los servidores, y por tal motivo inactividad total en tramitaciones administrativas de pago a proveedores y empleados
- **Robo:** pérdidas totales o parciales, según la gravedad de los hechos.
- **Virus informáticos:** generaría molestias en el sistema, ya que lo degradan y lo hacen más lento. Habría pérdidas totales o parciales, de la información almacenada.

- **Ataques internos:** generaría pérdidas totales o parciales, así como también, vulnerabilidad del sistema.

Los que afectan la integridad de los datos:

- **Los problemas de comunicación con los servidores:** Los problemas en el cableado eléctrico de las estaciones de trabajo, los problemas con los recursos compartidos de la red y la caída de la base de datos, ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema.
- **Caída temporal del o los servidores/es por falla mecánica:** ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema. Evaluar costo de reparación del desperfecto mecánico.
- **Pérdida total de un servidor:** ocasionaría pérdidas totales o parciales, por lo tanto, hay una interrupción en las actividades, hasta solucionar el problema, además evaluar costo de reparación o de reposición.
- **Falla total o parcial del cableado:** ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.
- **Pérdida total o parcial de las estaciones de trabajo:** ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema, en caso de pérdida total, evaluar costos.

ASIGNACIONES DE PRIORIDADES EN LAS APLICACIONES

A continuación, se detalla la lista de aplicaciones que posee la Institución, ordenada por la relevancia y prioridad. Las aplicaciones de máxima relevancia son las que deben estar en funcionamiento siempre.

Aplicación	Relevancia	Comentario
Sistema BOS	ALTA	Este Sistema es el más importante ya que maneja toda la administración financiera de la institución.
Sistema Specify	ALTA	Sistema que se encarga de manejar los pagos tantos para empleados como para proveedores institucionales.
Colecciones de patrimonio cultural	ALTA	Manejo de la información de las colecciones de patrimonio cultural

Aplicación	Relevancia	Comentario
Colecciones de patrimonio natural	ALTA	Manejo de la información de las colecciones de patrimonio natural
Investigaciones arqueológicas	ALTA	Manejo de la información de las investigaciones y de sitios arqueológicos

PROCEDIMIENTO DE RECUPERACIÓN

INCENDIO

¿Qué hacer?	**Previo al incidente:** Valorar e identificar o señalizar los equipos de importancia relevante para la institución con el fin de protegerlos del fuego, ya sea sacándolos de la institución o bien alejándolos del peligro.	**Durante el Evento:** Prevalece el respecto a la vida humana por lo que el principal objetivo es salir del edificio lo antes posible y alertar a las autoridades competentes para que se hagan cargo del siniestro.	**Después del Evento:** Realizar una valoración de los daños ocasionados durante el evento y tratar de poner en funcionamiento en el menor tiempo posible los equipos que no hayan reportado daños.
¿Cómo?	Mediante el etiquetado o codificación que deberá tener cada equipo de la institución se valorará la importancia del mismo, con el fin de priorizar los esfuerzos de rescate para determinado hardware o software.		
Responsable	Unidad de Informática.		
Recomendaciones	1. Contar con una ubicación segura para guardar respaldos de la información y de los sistemas en otro lugar fuera de la institución, por ejemplo, en una de las sedes. 2. Contar con alarmas contra incendios. 3. Seguros o pólizas contra incendios. 4. Puertas anti fuegos, o bien paredes con material anti fuegos. 5. Se recomienda realizar revisiones periódicas y mantenimiento de los extintores. 6. Publicar un plan de evacuación contra incendios donde se especifique las salidas de seguridad y hacer simulacros cada 6 meses. 7. Señalizar los equipos que deben ser rescatados en caso de que exista riesgo. 8. Realizar una prueba con los respaldos de las bases de datos, para saber si estas funcionarían en caso de perder los originales.		

FALTA DE FLUIDO ELÉCTRICO

¿Qué hacer?	Actualmente en la institución no se cuenta con una planta que se inicie cada vez que falta el fluido eléctrico; por lo tanto, es una necesidad que se plantea en el presente manual. Se deberá notificar de inmediato la falla de fluido eléctrico en la zona a la CNFL Estar pendiente de que las UPS que mantiene los equipos tales como servidores, no caduquen su tiempo de funcionamiento; ya que si esto sucede puede resultar grave para este tipo de hardware. Si no existe UPS y hay una falta de fluido eléctrico no se puede hacer nada ya que el corte en la corriente apaga inmediatamente la computadora por lo que se recomienda estar guardando cada 5 minutos los documentos que estén trabajando.
¿Cómo?	La comunicación debe darse de inmediato entre los responsables que se citan en el apartado de "Responsables", sea de forma personal o bien mediante la red telefónica para una correcta coordinación de la labor a realizar.
Responsable	Unidad de Informática.
Recomendaciones	1. Compras de UPS para las PC de los Departamentos, para evitar que fallen los equipos por corto circuito o picos de voltaje, que puedan quemar las fuentes de poder de los equipos. 2. Revisar el sistema eléctrico. De la misma forma se recomienda la revisión del cableado eléctrico, ya que las instalaciones en el edificio son antiguas. 3. Hacer una revisión de las lámparas de emergencia en la institución, y cambiar aquellas que se encuentren en mal estado y adquirir las que sean necesarias colocándolas en lugares estratégicos para la salida del personal y del equipo en caso de riesgo.

ROBO O FRAUDE

¿Qué hacer?	Notificar a la Unidad de Informática y a la Asesoría Jurídica lo sucedido. Si el equipo robado es de vital importancia para el correcto funcionamiento del Museo Nacional de Costa Rica, se procede a reemplazar el equipo de forma inmediata. De la misma forma si se diera un robo de información, se reemplaza o levanta la información de respaldo. Además, se debe realizar la denuncia respectiva al OIJ.

¿Cómo?	Debe quedar registrado de manera oficial el acto ilícito. Paralelamente se evalúa el impacto que tiene el equipo sustraído y cómo afecta el buen proceder de la institución. En caso de que el impacto sea alto, el equipo deberá sustituirse de manera inmediata. Esta valoración puede darse según el color que tiene etiquetado el hardware. **En caso de Robo: Se presentan varias situaciones** 1. Si la(s) persona(s) son sorprendidas en el momento del acto y ésta(s) se da(n) a la fuga, se debe realizar una llamada inmediata a los oficiales para que cierren el perímetro del Museo Nacional de Costa Rica. 2. Si el robo se descubre posterior al hecho, hay que notificar de manera oficial al área de informática; así como a la Dirección General con el fin de tomar medidas. a. Robo de equipo: Denuncia al OIJ. b. Robo de información: Denuncia al OIJ y verificación de respaldos en medios extraíbles.
Responsable	La persona que notase la irregularidad está en la obligación de notificar a su jefe inmediato.
Recomendaciones	1. Tener a mano los números telefónicos de los oficiales del Museo. 2. Se recomienda la segregación de funciones y aplicar las normas de control interno. 3. Control sobre los activos con inventarios periódicos sobre los mismos. 4. Seguridad física en el ingreso de personas ajenas al Departamento o la Institución. 5. Puertas de seguridad con acceso autenticado. 6. Nombrar a una persona exclusiva para controlar la calidad y seguridad en los datos. 7. Respaldos de la información tanto locales como fuera de la institución.

VANDALISMO Y/O TERRORISMO

¿Qué hacer?	De la misma manera del punto anterior se recomienda notificar a las autoridades pertinentes dentro de ellas, la seguridad local y denunciar el ilícito al OIJ
¿Cómo?	Para este caso en particular lo más importante es la prevención de estos hechos vandálicos. Dentro de las acciones más comunes están: 1. Haciendo respaldos. 2. Guardando los respaldos fuera de la institución.
Responsable	El Departamento de Administración y Finanzas es el responsable de la seguridad dentro de la institución. Para los efectos de los datos la Unidad de Informática será la encargada de levantar los respaldos.

ATAQUES DE VIRUS

¿Qué hacer?	Se cuenta con un software para antivirus llamado ESSET, el cual se está actualizando diariamente en Internet.
¿Cómo?	Avisar por medio de correo electrónico la existencia de un virus, por lo que se les indica no compartir archivos o carpetas, o en su defecto no introducir dispositivos de almacenamiento a las máquinas en esos momentos.
Responsable	Unidad de Informática
Recomendaciones	1. Bajar software de diagnóstico que vele porque los directorios que se encuentren compartidos tengan la seguridad adecuada. 2. Todas las máquinas del Museo Nacional deben tener el antivirus instalado de modo residente, con el fin de mejorar la seguridad en cada máquina.

DESASTRE NATURAL

¿Qué hacer?	Un desastre natural siempre es algo imprevisto para el cual debemos estar preparados. En caso de que el desastre afecte al Museo Nacional de Costa Rica, se debe tener una copiar fiel de los datos en una ubicación fuera de la sede central.
Responsable	Unidad de Informática

DAÑOS PARCIALES DE EQUIPOS

¿Qué hacer?	Tener asegurados los equipos como servidores y los equipos de telecomunicación.
¿Cómo?	Se deben realizar contratos de mantenimiento para los equipos de comunicación que hay en esta institución. En el caso de los equipos que se encuentran en el cuarto de servidores se cuenta con aire acondicionado, con el fin de protegerlos de las inclemencias del tiempo, también se cuenta con UPS para los equipos, con el fin de evitar fallos de fluido eléctrico, como ya se mencionó anteriormente. Si uno de estos equipos fallara lo que se deberá hacer es: llamar inmediatamente al proveedor de los equipos para que se realice la negociación respectiva y cambiar el equipo. Se debe contar con los números telefónicos de las personas o entidades necesarias para realizar el cambio.
Responsable	Unidad de Informática
Recomendaciones	1. Tener contratos de mantenimiento para los equipos. 2. Tener seguros que protejan los equipos de telecomunicación. 3. Acceso restringido al sitio donde se encuentran los equipos

FALLAS NORMALES DEL EQUIPO

¿Qué hacer?	Plan de mantenimiento preventivo de los equipos de la institución tales como limpieza, revisión, chequeo de cargas de trabajo.
¿Cómo?	1. Identificar el problema de manera inmediata. 2. Una vez identificado, evaluar el impacto de que el equipo no esté funcionando y si los servicios que brinda la institución se detendrán 3. De ser un servicio que pertenece al grupo de prioridad alta sustituir el equipo y restaurar el equipo. 4. Enviar el equipo a soporte técnico para una evaluación más detallada del daño sufrido por el equipo.
Responsable	Unidad de Informática
Recomendaciones	1. Asegurar los equipos 2. Contrato de mantenimientos a equipos como routers y servidores 3. Plan de mantenimiento preventivo y correctivo del equipo. 4. Adquirir equipo para trabajo pesado tal es el caso de impresoras que soportan cargas de trabajo altas de la misma manera computadoras, servidores y equipo en general de comunicaciones tal como routers o switch.

RECOMENDACIONES GENERALES.

1. Contar con mecanismos alternativos de acceso a la red fuera del edificio.
2. Realizar respaldos de los sistemas de información actualizados fuera de la institución.
3. Realizar respaldos de las bases de datos fuera de la institución.
4. Mantener procedimientos para actualizar los sistemas que están de respaldo cada vez que se hagan modificaciones o mantenimientos a los sistemas.