

MUSEO NACIONAL DE COSTA RICA

Dirección General

Unidad de Informática



Normas Institucionales sobre Tecnologías de Información del Museo Nacional de Costa Rica

**MUSEO NACIONAL
DE COSTA RICA**

Elaborado por:

Unidad de Informática

Junio, 2019

APROBADO POR JUNTA ADMINISTRATIVA DEL MNCR

*EN EL ACUERDO A-19-1332, DE LA SESIÓN NÚMERO: 1332,
DEL DÍA 28 DEL MES DE JUNIO DEL 2019*

TABLA DE CONTENIDO

Introducción	3
Objetivo	3
Alcance	3
Consideraciones generales	3
Planificación y organización	4
Unidad de informática	4
Objetivo general:	4
Objetivos específicos	5
Lineamientos generales.....	5
Desarrollo de sistemas.....	6
Adquisición de tecnologías de información y de servicios profesionales.....	7
Uso del "software"	8
Uso del hardware	9
Acceso a la red interna e internet	10
Acceso y uso al servicio de correo electrónico	11
Uso de equipos portátiles de tecnologías de información	13
Información.....	14
Uso del portal "web" del museo.....	16
Uso de redes sociales por parte de los funcionarios.....	17
De la auditoría interna	17
Sanciones.....	17
Anexo 1	18

INTRODUCCIÓN

El mejoramiento en el poder computacional y las capacidades de ínter-conectividad de las tecnologías de información utilizada actualmente por cada uno de los diferentes funcionarios en el Museo Nacional de Costa Rica, hacen que su operación adecuada revista una mayor importancia, principalmente debido a las implicaciones negativas sobre la operación normal de la institución que podrían suceder por una mala utilización de las tecnologías de información.

Es por eso que se hace imperativo la definición de una serie de normas claras que regulen el uso apropiado de estas tecnologías, garantizando niveles adecuados de seguridad y minimizando las posibilidades de ataques por parte de terceras personas, ajenas o no a la organización, las cuales aprovechan las vulnerabilidades inherentes a la tecnología y a la falta de normas para realizar sus acciones.

En este manual institucional de normas para el uso de las tecnologías de información se emiten una serie de normas que han sido elaboradas en base a estándares internacionales, lineamientos de control interno, seguridad y demás documentos que regulan y rigen las labores de los funcionarios públicos.

OBJETIVO

Garantizar el uso correcto de los equipos de tecnologías de información y la instalación del software autorizado acorde a las funciones correspondientes de cada usuario.

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.

CONSIDERACIONES GENERALES

- a)** El personal del Museo Nacional debe de estar comprometido con las regulaciones de seguridad y confidencialidad que a continuación se detallan, con el fin de reducir los riesgos de error humano, físico, robo, fraude o uso inadecuado de los recursos de tecnologías de información.

- b)** Este documento establece la normativa macro sobre seguridad de la información. La seguridad de la información es la comprensión, conciencia y compromiso del personal del Museo Nacional de Costa Rica sobre la importancia de incorporar en sus prácticas cotidianas de gestión, un conjunto de controles (políticas y procedimientos).
- c)** El objetivo de la seguridad de la información es preservar las características de confiabilidad, integridad, confidencialidad, disponibilidad y cumplimiento de la información que utiliza, con el fin de respaldar sus procesos de misión crítica, como medio para asegurar la continuidad de las operaciones.
- d)** El alcance de la seguridad de la información está definido por los recursos tecnológicos: datos, tecnología, aplicaciones, instalaciones y capital humano.
- e)** El cumplimiento de estas normas es obligatorio. La naturaleza de las faltas asociadas con su incumplimiento y las eventuales sanciones, serán normalizadas institucionalmente por las instancias competentes.
- f)** Los jefes y el personal en general son los responsables de brindar la seguridad de la información mediante la promulgación, mantenimiento y divulgación de un manual de normas.

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.

LINEAMIENTOS GENERALES

Artículo 1. — El presente reglamento regulará lo relacionado con las políticas y lineamientos generales en materia de tecnologías de información y su utilización por parte de los funcionarios del Museo Nacional de Costa Rica, con el propósito de garantizar la eficiencia de la administración, el buen uso y aprovechamiento de tales tecnologías.

El proceso de inducción de los funcionarios de primer ingreso debe incluir la lectura de las mismas.

Artículo 2. — Se considerarán funcionarios del Museo Nacional de Costa Rica, todos aquellos que se encuentren al servicio de la institución, sea en la función administrativa y los servidores de temporales, protegidos o no por el Estatuto de Servicio Civil.

Artículo 3. — Todo funcionario del Museo Nacional de Costa Rica deberá respetar las políticas y lineamientos generales que se establecen en el presente cuerpo normativo,

en cuanto al uso, aprovechamiento y custodia de las tecnologías de información que se facilita para el desempeño de las funciones.

Artículo 4. — En cuanto a lo no regulado en las presentes disposiciones, se aplicará supletoriamente, en lo que corresponda: La Ley General de la Administración Pública, el Código de Trabajo, Estatuto de Servicio Civil y su reglamento, el Reglamento Autónomo de Servicios del Museo Nacional de Costa Rica, así como cualquier otra reglamentación vigente del Museo Nacional de Costa Rica.

La Unidad de Informática deberá contar con los procedimientos o protocolos institucionales para el cumplimiento de las “Normas técnicas para la gestión y el control de las tecnologías de información” de la Contraloría General de la República.

DESARROLLO DE SISTEMAS

Artículo 5. — La Unidad de Informática enviará en el segundo trimestre de cada año, invitación a las jefaturas de las diferentes dependencias del Museo, para que presenten las solicitudes de automatización de sus procesos en caso de que lo requieran.

Artículo 6. — Cada jefatura de las diferentes dependencias del Museo informará por escrito a la Unidad de Informática, de las necesidades de automatización de sus procesos.

Artículo 7. — Las solicitudes de automatización que se presenten deberán indicar, con la mayor precisión posible, la necesidad que se requiere satisfacer, y constituirán insumo a la Unidad de Informática para la elaboración del plan anual operativo del periodo siguiente.

Artículo 8. — Solo en caso de extrema urgencia o necesidad institucional y debidamente justificado por la jefatura de la dependencia interesada, la Comisión de Informática podrá autorizar, por vía de excepción, el desarrollo de un sistema para una determinada dependencia ministerial sin que se encuentre dentro del plan de trabajo de la Unidad de Informática. En tal supuesto, deberá documentarse la realización del proyecto priorizado como logro alcanzado en sustitución de alguno de los otros que no se pudieran realizar en razón de la alteración al plan anual operativo.

Artículo 9. — La Unidad de Informática deberá llevar registro de los sistemas de información que se desarrollen, así como de los cambios o actualizaciones realizadas.

Artículo 10. — Queda totalmente prohibido a las jefaturas de cualquier dependencia del Museo, como a los funcionarios en general, autorizar o en su caso desarrollar sistemas de automatización de procesos en los equipos de tecnologías de información propiedad del Museo, sin contar con la autorización previa de la Unidad de Informática.

ADQUISICIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y DE SERVICIOS PROFESIONALES

Artículo 11. — Para la adquisición de equipos de tecnologías de información o bien, de servicios profesionales temporales, el encargado del Departamento interesado solicitará por escrito a la Unidad de Informática la compra de equipos, licencias de “software” o la contratación de servicios profesionales.

Para tal efecto en la solicitud deberá justificar de manera detalla la necesidad existente para dicha adquisición o contratación y señalar los beneficios que traerá para la eficiencia del trabajo que desarrolla la dependencia a su cargo.

Artículo 12. — Corresponderá a la Unidad de Informática realizar el respectivo estudio técnico de las necesidades reales en materia de tecnologías de información de la dependencia solicitante. Realizado el estudio técnico respectivo, se remitirá el informe al encargado de la oficina solicitante, con las especificaciones técnicas de los equipos a adquirir y las cotizaciones respectivas.

Artículo 13. — En caso de compra de equipos de tecnología de información se debe incluir desde el inicio del análisis técnico, la distribución que se hará de los bienes por adquirir, lo cual deberá respetarse a la hora de realizar la asignación de los equipos adquiridos a las diferentes dependencias.

Artículo 14. — En los casos de que se trate de un proyecto a nivel institucional o de gran impacto, la Unidad de Informática deberá llevar la documentación respectiva a la Comisión de Informática para su revisión y posterior aprobación.

Artículo 15. — Realizados los procedimientos de compra respectivos, luego de que la Unidad de Informática haya aceptado los bienes a satisfacción, la oficina de control de activos procederá a patrimonializar los equipos de tecnología de información adquiridos, previo a autorizarse su salida.

Artículo 16. — Una vez patrimonializado el equipo adquirido, la Unidad de Informática procederá a retirarlos para la configuración respectiva y posterior entrega a la dependencia a quien corresponde la asignación del equipo, conforme la previsión hecha desde el principio del trámite.

Artículo 17. — En todos los casos de adquisición de equipos de tecnologías de información por compra, la Unidad de Informática deberá resguardar copias de las facturas y garantías.

Artículo 18. — En caso de potenciales donaciones de equipos de tecnología de información al Museo, el órgano competente deberá solicitar a la Unidad de

Informática, un estudio de factibilidad de los equipos o el "software" que se quieran donar, en el que se analice si está acorde con la plataforma tecnológica del Museo, así como los aspectos de garantía de los equipos, recursos que requieren para su mantenimiento, su licenciamiento, entre otros.

Artículo 19. — Por aceptada la donación por parte del órgano institucional competente al efecto, se procederá a realizar el ingreso de los bienes, registrarlos y patrimonializarlos, así como impregnarles el código o número de patrimonio correspondiente.

Artículo 20. — En el caso que los bienes donados sean para una finalidad o dependencia determinada, se procederá a su entrega según lo previsto. De lo contrario, la Unidad de Informática procederá a realizar un estudio de necesidades de las diferentes unidades para su asignación.

Artículo 21. — En el caso de la contratación de servicios profesionales o consultorías se aplicarán las disposiciones anteriores en lo que resulte pertinente; no obstante, en todos los casos deberá contarse con la aprobación previa de la Unidad de Informática.

Se formalizará un contrato para cada consultoría conteniendo claramente los términos en los que esta habrá de desarrollarse.

La Unidad de Informática establecerá los mecanismos de control necesarios para asegurar el cumplimiento de los requerimientos establecidos en los diferentes contratos formalizados.

USO DEL "SOFTWARE"

Artículo 22. — La única dependencia autorizada para instalar y desinstalar "software" en los equipos y dispositivos de tecnologías de información del Museo Nacional de Costa Rica, será la Unidad de Informática a través de sus funcionarios autorizados.

Artículo 23. — El "software" que se utilice deberá ser principalmente el que adquiera el Museo por medio de los procedimientos legales establecidos al efecto. No obstante, podrá utilizarse "software" de licencia libre en los equipos, siempre y cuando sean de utilidad para las labores propias de las dependencias correspondientes, previa revisión y comprobación por parte de la Unidad de Informática. De igual forma, si se trata de "software" que permita alguna facilidad mayor para el mejor desempeño de los funcionarios en casos especiales.

Artículo 24. — La utilización del “software” será para el desempeño de las labores habituales de los funcionarios usuarios, para el logro de los objetivos y cumplimiento de las funciones que corresponden a la dependencia en que labora.

Artículo 25. — Ningún funcionario podrá realizar copias o respaldo del “software” que pertenezca al Museo; instalar o desinstalar “software” o aplicaciones en violación a los términos de las licencias adquiridas por el Museo; borrar o cambiar archivos de los sistemas o configuraciones de los equipos que le han sido asignados, sin que medie la intervención del personal autorizado de la Unidad de Informática.

Artículo 26. — Todo el “software” original contenido en cintas, discos compactos, discos de video digital u otro medio de almacenamiento, deberá ser custodiado por la Unidad de Informática.

La Unidad de Informática deberá mantener un inventario actualizado de licencias de “software” con indicación de los equipos en que se encuentren instalados.

Artículo 27. — Ningún funcionario del Museo podrá accesar, guardar, reproducir, observar o exhibir material pornográfico.

Lo anterior sin perjuicio de que en razón de las funciones que se desempeñan de conformidad con la competencia delegada, se deba tener contacto con material de ésta naturaleza.

USO DEL HARDWARE

Artículo 28. — A todo funcionario autorizado por la Jefatura de la oficina o unidad laboral se le asignará una cuenta de acceso de usuario y contraseña al equipo de tecnologías de información, la cual es intransferible, por lo que deberá adoptar las medidas necesarias para mantener en secreto su clave de acceso y será el responsable por el uso que se le dé a la cuenta. Asimismo, solo podrá utilizar la cuenta propia que le ha sido asignada.

En caso de cese de funciones o de traslado del funcionario a otra oficina o unidad laboral, el Jefe deberá informar a la Unidad de Informática, para la cancelación de la cuenta de acceso de usuario y contraseña del equipo que tenía asignado.

Artículo 29. — Todos los equipos y dispositivos de tecnologías de información del Museo Nacional de Costa Rica, deberán ser instalados, reubicados, configurados, revisados y desmantelados, únicamente por los funcionarios autorizados de la Unidad de Informática, quienes deberán llevar control de los cambios realizados y actualizar el inventario de las licencias de “software” cuando así lo amerite.

Artículo 30. — Ningún funcionario podrá reubicar o reconfigurar los equipos de las tecnologías de información que le han sido asignados para su desempeño laboral o de la oficina, sin que medie la intervención del personal autorizado de la Unidad de Informática.

Artículo 31. — De requerirse el traslado de los dispositivos o equipos de las tecnologías de información en diferente locación dentro de la misma oficina o bien de una oficina a otra, se debe comunicar con anticipación a la Unidad de Informática para que los funcionarios competentes procedan a realizar la desinstalación del equipo, la instalación y las configuraciones pertinentes y demás tareas que resulten necesarias.

Artículo 32. — Los equipos o dispositivos de tecnologías de información del Museo deberán ser utilizados en labores propias del cargo y dentro de los horarios autorizados. No se deben utilizar para asuntos personales ajenos al trabajo, ni en perjuicio de las labores que deben realizarse.

Artículo 33. — Ningún funcionario podrá comer, beber, o tener alimentos, ni líquidos en los sectores donde se ubican los equipos de tecnología de información.

Artículo 34. — Los funcionarios usuarios de los equipos de tecnologías de información del Museo deberán velar por el cuidado de los mismos y reportar a la Unidad de Informática cualquier falla que se detecte a efectos de que se realicen las reparaciones o ajustes que corresponda a la mayor brevedad posible, con la finalidad de mantenerlos en condiciones óptimas de funcionamiento.

ACCESO A LA RED INTERNA E INTERNET

Artículo 35. — A todo funcionario autorizado por la Jefatura de la oficina o unidad laboral en que labora se le asignará una cuenta de acceso a Internet y será el responsable por el uso que se le dé a la cuenta.

El ingreso a páginas restringidas solo podrá ser brindado por la Unidad de Informática, previa autorización escrita por el Jefe respectivo, indicando el nombre del funcionario, número de cédula y la debida justificación.

Para tales efectos la Jefatura respectiva hará la solicitud correspondiente a la Unidad de Informática.

Artículo 36. — Los funcionarios del Museo solo podrán acceder de manera remota a los equipos de tecnologías de información de otros funcionarios, que le hayan sido autorizados previamente, conforme los accesos realizados por la Unidad de Informática.

Artículo 37. — Los funcionarios del Museo solo podrán utilizar las conexiones vía FTP o de conversación en línea MSN, u otras de similar utilidad, cuando así se le haya autorizado previamente y la Unidad de Informática haya instalado y configurado el “software” necesario con el perfil de acceso respectivo.

Tampoco podrá utilizarse ningún otro tipo de “software” que no sean los exploradores autorizados e instalados por la Unidad de Informática, para acceder Internet.

Artículo 38. — No se podrán utilizar los equipos de tecnología de información del Museo para proferir amenazas o cualquier tipo de acoso a personas dentro o fuera del Museo, emitir mensajes reñidos con los valores institucionales, falsificar o utilizar una identidad que no sea la propia, utilizar los recursos con fines recreativos o afectar el ancho de banda con la descarga de archivos de música, imágenes, videos u otros de similar naturaleza.

ACCESO Y USO AL SERVICIO DE CORREO ELECTRÓNICO

Artículo 39. — A todo funcionario autorizado por la Jefatura de la oficina o unidad laboral en que labora se le asignará una cuenta de correo electrónico en el servidor de la Institución. Se asignará solamente una cuenta por usuario.

Las cuentas por proyectos o temporales, se asignarán a consideración de la Unidad de Informática.

Para tales efectos la Jefatura respectiva hará la solicitud correspondiente a la Unidad de Informática.

En caso de cese de funciones del funcionario, el Jefe deberá informar a la Unidad de Informática, para la cancelación de la cuenta de correo electrónico.

Artículo 40. — La vigencia de la cuenta será por el periodo en que la persona labore para la Institución. Los espacios de almacenamiento de las cuentas serán definidos por la Unidad de Informática de acuerdo con los recursos disponibles y con base en las necesidades del usuario.

El funcionario que tenga asignada una cuenta de correo electrónico, deberá adoptar todas las medidas necesarias de previo a la terminación de la relación laboral, a efectos de recuperar la documentación de los correos electrónicos de su interés, así como de informar a sus contactos electrónicos, según lo estime pertinente, de su nuevo medio para recibir la comunicación personal.

No obstante, lo anterior, habrá un periodo de dos meses de gracia, contados a partir de la fecha de terminación de la relación laboral, a efectos de que el exfuncionario

pueda realizar la copia de la información contenida en su correo electrónico institucional. Pasados los dos meses de terminada la relación de servicio, la Administración procederá a la cancelación del acceso y la cuenta a nombre del exfuncionario.

Artículo 41. — Las cuentas de correo asignadas son para uso institucional y no son transferibles, no debe permitirse que terceras personas hagan uso de ella. Los funcionarios autorizados deben utilizar el correo electrónico asignado únicamente para comunicaciones cuyo fin sea lícito, ético y de provecho para el Museo, para efectos laborales, académicos o institucionales.

Artículo 42. — Los correos masivos se realizarán para aquellos funcionarios o instancias que por sus funciones así lo requieran. El interesado deberá presentar solicitud a la Unidad de Informática para la asignación del perfil respectivo para realizar el envío respectivo.

Artículo 43. — El usuario puede enviar correos a las listas de distribución creadas por la oficina o unidad laboral y en su defecto podrá mantener su propia libreta de contactos personales, siempre y cuando dicha libreta no interfiera con las políticas del presente reglamento, ni con el funcionamiento del Servidor de Correos.

Al responder comunicados generales o para un grupo específico de usuarios, el usuario deberá cuidar de no responder a todos los usuarios, salvo cuando ésta sea la finalidad de la respuesta, procurando evitar el envío y contestación de cadenas de correo y no enviar correos a destinatarios que no los han solicitado.

Artículo 44. — El servicio de correo electrónico no se puede usar como medio para entablar discusiones o conversaciones tipo “chats” sobre temas que no sean laborales; ni debe utilizarse la cuenta de correo para la creación de perfiles o para registrarse en redes sociales como “Facebook”, “Twitter”, “sónico”, “badu”, “Linkedin”, “Myspace”, “Slideshare”, “Windows Live Profile” u otras de similar naturaleza.

Artículo 45. — El usuario es responsable de la información que envía desde su cuenta o hace llegar a su cuenta institucional, por lo cual deberá asegurarse de hacer un uso racional del servicio y no enviar archivos adjuntos que pudieran contener información nociva, peligrosa u ofensiva, tales como virus informáticos, mensajes insultantes o pornográficos u otros de similar naturaleza.

Artículo 46. — La Unidad de Informática podrá monitorear mediante “software” preventivo, las cuentas que presenten un comportamiento irregular para la seguridad del Museo, sin que ello signifique que pueda leerse el contenido del mensaje. Asimismo, podrá realizar chequeos sobre la procedencia de los correos electrónicos

de manera que cancelará aquellos que se consideren inseguros, notificando al usuario de la anomalía encontrada.

Artículo 47. — El usuario es responsable de respaldar sus archivos de correo manteniendo en la bandeja de entrada solamente documentos en tránsito; sus demás comunicados deberán mantenerlos en una carpeta personal en su computador local y depurar su "bandeja de entrada o "Inbox", al igual que las bandejas de elementos eliminados y enviados, para no saturar el buzón.

Artículo 48. — El usuario es responsable de respetar la ley de derechos de autor, por lo que no debe abusar de este medio para distribuir en forma ilegal "software" licenciado o reproducir información sin conocimiento del autor.

Artículo 49. — El usuario será responsable de mantener la confidencialidad de la contraseña y de la cuenta de correo electrónico que se le asigne y será el responsable por las actividades que se realicen con su cuenta de correo.

Artículo 50. — Será responsabilidad del usuario hacer buen uso de la cuenta de correo electrónico, entendiendo por buen uso, además de lo ya indicado, lo siguiente:

- a) No hacer uso de la cuenta de correo electrónico para fines comerciales, personales o familiares.
- b) Respetar las cuentas de otros usuarios internos y externos y no comprometer su privacidad.
- c) Preocuparse por el correcto uso del lenguaje en cuanto a estilo, redacción, ortografía y vocabulario apropiado, en tutela de la imagen de la Institución.

USO DE EQUIPOS PORTÁTILES DE TECNOLOGÍAS DE INFORMACIÓN

Artículo 51. — Los dispositivos o equipos portátiles de tecnologías de información deben utilizarse únicamente para efectos laborales institucionales, por lo que no se permite para el trasiego de información personal; asimismo, no debe permitirse su uso por parte de terceras personas.

Artículo 52. — Los funcionarios a quienes se les asigne dispositivos o equipos portátiles de tecnologías de información, tales como Laptop, tabletas u otros, deberán adoptar al menos las siguientes medidas de seguridad:

- a) Velar por la debida custodia del dispositivo o equipo portátil asignado, por lo que deberá mantenerlo siempre a la vista para su cuidado.

- b) No utilizarlo ni ubicarlo en lugares en donde puedan correr riesgo de daño físico o de funcionamiento y evitar la cercanía de alimentos, líquidos u otros elementos que puedan afectarlo.
- c) Proteger con contraseña el acceso al dispositivo de tecnología de información asignado.
- d) Mantener sus carpetas y archivos importantes con contraseñas y ocultas, si es posible incluso encriptados.
- e) Respaldo periódicamente los archivos y la documentación oficial de la Institución conforme se requiera; pero en todo caso deberá hacerse el respaldo de la información al menos una vez al mes y si se trata de información altamente sensible deberá realizarse diariamente.

Artículo 53. — No se debe conectar automáticamente a redes inalámbricas abiertas para evitar conectarse a uno falso y poner en riesgo el acceso no autorizado y la sustracción de la información que contenga.

Artículo 54. — Someter periódicamente a control y revisión ante la Unidad de Informática el dispositivo portátil asignado para verificar que cuenta con los mecanismos de seguridad, tales como "software antivirus", debidamente habilitados y actualizados.

Artículo 55. — Si los dispositivos de tecnología de información asignados cuentan con "bluetooth" deben adoptarse al menos la siguiente medida preventiva:

- a) Deshabilitar la función de conexión vía "bluetooth" cuando ésta no se utilice o en sitios públicos o muy concurridos. Lo anterior para evitar conexiones y transferencias de información no autorizados y alargar el tiempo de uso de la batería.

Artículo 56. — Únicamente se podrá conectar con otros dispositivos móviles de sincronización, tales como agendas electrónicas, teléfonos inteligentes, tabletas u otros con los que se puedan realizar intercambios de información, si están autorizados de forma explícita por la jefatura de la unidad respectiva conjuntamente con la Unidad de Informática.

INFORMACIÓN

Artículo 57. — La Unidad de Informática será la responsable de resguardar las Bases de Datos que contengan información generada en las distintas oficinas o unidades laborales de la Institución; no obstante, el acceso a la información respectiva por

parte de terceros, solo podrá ser autorizada por la oficina o dependencia responsable de generar los datos contenidos.

Artículo 58. — Todo funcionario del Museo Nacional de Costa Rica que tengan asignado algún dispositivo o equipo de tecnología de información para el desempeño de sus labores, está en la obligación de respaldar periódicamente los datos y la información oficial que se ha producido para la Institución conforme se requiera; pero en todo caso deberá hacerse el respaldo de la información al menos una vez al mes y si se trata de información altamente sensible deberá realizarse diariamente.

En aquellos casos, en que el usuario no cuente con el dispositivo para grabar, puede optar por utilizar una unidad "CD-RW" ó "DVD-RW" compartida, que se encuentre ubicado en la misma dependencia.

El usuario encargado de tal obligación deberá responder por los daños y perjuicios ocasionados por la pérdida de información imputable a título de dolo o culpa, previo cumplimiento del debido proceso administrativo.

Artículo 59. — Si por alguna circunstancia, el usuario debe entregar un dispositivo o equipo de tecnología de información, será responsable por la información sensible, confidencial o crítica que el equipo pueda contener. De ser factible moverá esa información, sea por medio físico o electrónico, a otro medio de almacenamiento. Para realizarlo, solicitará a la Unidad de Informática el asesoramiento respectivo.

Artículo 60. — En el caso de que se deba proceder con la eliminación de toda la información del computador (Formateo de Disco Duro) debido a que se haga imposible la reparación del Sistema Operativo contenido en el equipo, se coordinará con los usuarios del equipo para determinar si tiene respaldo reciente o si no le fue posible realizarlo por las condiciones del equipo; en dicho caso, el usuario deberá indicar qué información debe ser respaldada por parte de técnico a cargo de la reparación.

La información que se respaldará será únicamente la de carácter oficial, que el usuario indicará al técnico responsable de la reparación por medio de oficio o correo electrónico, indicando en donde se ubican los datos que deben respaldarse.

Artículo 61. — El funcionario que, por motivos de aprovechamiento de incapacidad médica, disfrute de vacaciones o autorización de licencia, deba ausentarse de la oficina por más de dos días, estará en la obligación de suministrar a su Jefe inmediato, copia de la información oficial que esté contenida en el equipo asignado; así como aquella que esté en proceso de elaboración.

Artículo 62. — Cada funcionario usuario debe bloquear el equipo de tecnología de información asignado, cuando no lo vaya a utilizar o se aleje del mismo

circunstancialmente, con la finalidad de evitar su utilización no autorizada por parte de terceras personas.

Artículo 63. — De previo al traslado del funcionario a otra oficina o unidad laboral, o a la terminación de la relación laboral con el Museo, el funcionario deberá realizar un respaldo de la información digital generada para la Institución contenida en su dispositivo o equipo y entregarlo a su jefatura. Asimismo, deberá resguardar su documentación personal y eliminarla del equipo que tenía asignado.

No obstante, lo anterior, habrá un periodo de gracia de dos meses, contados a partir de la fecha de su traslado o de la terminación de la relación laboral, para que pueda realizar la copia de su información personal contenida en el equipo que tenía asignado, así como para realizar su respectiva eliminación, en caso de que por alguna circunstancia no lo hubiera realizado oportunamente.

Pasados los dos meses establecidos, La Unidad de Informática procederá a la cancelación del acceso y la eliminación de la cuenta a nombre del exfuncionario.

DEL USO DEL PORTAL “WEB” DEL MUSEO

Artículo 64. — El Museo contará con un portal “web” único, que debe incluir a todas los Departamentos y Programas. Ninguna dependencia podrá tener su propia página “web” separada del portal Institucional.

Artículo 65. — La Unidad de Informática en conjunto con la Jefatura de cada dependencia, designarán a las personas que fungirán como gestores del contenido de la información que se publicará y actualizará en el portal “web”.

Artículo 66. — Se contará con un gestor de contenido principal que deberá ser un funcionario del Departamento de Proyección Museológica, quien deberá coordinar lo pertinente con los demás gestores que se designen en las diferentes dependencias y determinará la información que deberá publicarse en el portal “web” del Museo.

Artículo 67. — La Unidad de Informática les asignará a los gestores de contenido un perfil de usuario y contraseña de uso personal, por lo que deberán adoptar las medidas necesarias para mantener su contraseña o clave de acceso en secreto, quedando como responsables por el uso que se le dé a la cuenta.

Artículo 68. — La Unidad de Informática deberá brindar la capacitación respectiva para la operación del “software” a los gestores de contenido del portal “web”.

USO DE REDES SOCIALES POR PARTE DE LOS FUNCIONARIOS

Artículo 69. — Todos los funcionarios del Museo Nacional de Costa Rica, en general, deberán abstenerse de utilizar los equipos de tecnología de información y demás recursos que dote el Museo, para acceder a sus perfiles personales en los medios de redes sociales digitales durante las horas laborales.

Únicamente podrán hacerlo los funcionarios previamente autorizados por la Jefatura de la Dependencia de que se trate, conjuntamente con la Unidad de Informática, para efectos estrictamente laborales.

Artículo 70. — Igualmente, todos los funcionarios del Museo Nacional de Costa Rica deberán abstenerse de publicar, exhibir o propalar, en sus perfiles personales de los medios de redes sociales digitales, información sensible de la unidad en que laboran o de cualquier otra dependencia del Museo, que comprometan la operatividad y funcionalidad institucional; o bien, imágenes, información o expresiones que afecten o puedan afectar o poner en entredicho el buen nombre y la buena imagen del Museo Nacional de Costa Rica. Asimismo, deberán de abstenerse de utilizar tales medios personales, para proferir ofensas contra compañeros de trabajo, subalternos y superiores.

DE LA AUDITORÍA INTERNA

Artículo 71. — La Auditoría Interna podrá realizar las verificaciones que estime pertinentes en relación con el correcto uso de los equipos de tecnologías de información, licencias de “software” e información pública contenida en los equipos de tecnologías de información, de conformidad con su competencia y atribuciones establecidas en la Ley de Control Interno y demás disposiciones legales y reglamentarias relacionadas.

Para tales efectos se deberá tener en cuenta las limitaciones propias del secreto de las comunicaciones y la inviolabilidad de los documentos privados, por lo que deberá accederse a los equipos en presencia del respectivo funcionario.

SANCIONES

Artículo 72. — El incumplimiento de las disposiciones del presente cuerpo normativo, por parte de algún funcionario, podrá derivar en sanciones según se indique en el Reglamento Autónomo de Servicio del Museo Nacional de Costa Rica.

ANEXO 1

DIRECTRICES DE USO Y CREACIÓN DE CONTRASEÑAS

- 1.** Los passwords o contraseñas secretas son utilizados para varios propósitos. Algunos de los usos más comunes incluyen: cuentas al nivel de usuario, cuentas de correo y para acceder a carpetas de redes locales.
- 2.** Evitar las siguientes prácticas en las contraseñas:
 - a.** Menos de ocho caracteres o palabra encontrada en un diccionario.
 - b.** Palabra de uso común: nombres de familia, mascotas, amigos, compañeros, o fábulas. o Términos y nombres de computadoras, comandos, sitios, compañías, hardware, software. o Fechas de cumpleaños y otra información personal como direcciones y números de teléfono.
 - c.** Patrones de números y letras como aaabbb, qwerty, zyxwvuts, y 123321.
 - d.** Cualquiera de las de arriba deletreadas, al revés.
 - e.** Cualquiera de las de arriba señaladas, precedidas o seguidas por un dígito (Ej.: secreto1, 1secreto)
- 3.** Las contraseñas deben contar con las siguientes características:
 - a.** Deben contener letras en mayúscula y en minúscula (Ej.: a-z, A-Z)
 - b.** Deben contener dígitos y caracteres de puntuación, así como letras, por ejemplo, 0-9, !@#\$%^&*()_+|~=\`{ } [] : " ; ' < > ? , . /)
 - c.** Deben ser de por lo menos ocho caracteres alfanuméricos.
- 4.** Se debe velar por la protección de las contraseñas, por lo tanto:
 - a.** No lo escriba en papel ni lo almacene en su oficina.
 - b.** No almacene esta contraseña en NINGUNA computadora de la oficina
 - c.** No se permite compartir las contraseñas del Museo Nacional de Costa Rica con nadie. Todas las contraseñas deben ser tratadas como sensitivas y de información confidencial del Museo Nacional.
 - d.** No revelar una contraseña en una conversación telefónica o mensaje de correo.
 - e.** No revelar una contraseña a terceras personas.
 - f.** No hablar de una contraseña en frente de otros.
 - g.** No revelar una contraseña en un cuestionario o formularios de seguridad.
 - h.** No revelar una contraseña a un compañero de trabajo mientras está de vacaciones.