Departamento de Informática

DI-PO 02-2014

Política
Integral de Seguridad de la Información

Fecha de envío:
Enero, 2014

TABLA DE CONTENIDOS

Aspectos Introductorios de las Políticas de Seguridad de la Información

1. Objetivos

Este documento tiene como objetivos principales:

1. Guiar sobre las conductas esperadas en materia de seguridad de la información.
2. Concienciar sobre los riesgos en materia de seguridad y las medidas a tomar para administrar adecuadamente dichos riesgos.
3. Esclarecer la responsabilidad y los deberes de los distintos actores en la protección de los recursos informáticos.
4. Empoderar al personal usuario para la toma de decisiones asertivas en materia de protección de los sistemas tecnológicos y de información.
5. Educar sobre el papel activo que deben desempeñar los distintos actores en la estructura de seguridad de la información del Ministerio de Cultura y Juventud (en adelante denominado también "el MINISTERIO DE CULTURA Y JUVENTUD", "Ministerio" o "MCJ");
6. Alertar sobre la necesidad de que:

    a) Se cumpla con los requisitos legales y contractuales aplicables al Ministerio;
    b) Se cumpla con los requerimientos de capacitación adecuados a las necesidades del Ministerio;
    c) Se manejen, prevengan y detecten en su debido tiempo, instrucciones maliciosas que puedan llegar a afectar los sistemas informáticos de la Institución;
    d) Se prevean acciones para mantener en todo momento la continuidad de los servicios; y
    e) Se tomen acciones en caso de violaciones a la normativa de Seguridad.

2. Alcance

Las PSI **protegen toda la información de interés** para El Ministerio de Cultura y Juventud y/o a los Administrados:

a) Sin importar su formato (e.g. oral, escrita, electrónica, digital, imágenes entre otras);
b) Sin importar los canales por los cuales se maneja (e.g. bases de datos, archivos, equipo computacional de cualquier naturaleza, registros, máquinas contestadoras, teléfonos –incluyendo teléfonos inteligentes-, máquinas de fax; organizadores personales y redes internas y externas, entre otras);

c) Independientemente del lugar en que físicamente se halle (e.g. en las oficinas del Ministerio de Cultura y Juventud, en lugares habilitados para teletrabajo, en los sitios web de la Institución y/o de los Administrados, entre otros);
d) Durante todo el ciclo de manejo de la misma (e.g. creación, inserción en los sistemas, procesamiento, transporte, diseminación, transmisión, custodia, y destrucción o devolución de la misma); y
e) Así como los equipos y aplicaciones que se utilicen para su manejo.

Las PSI son de carácter obligatorio y deben ser aplicadas sin excepción, por todo el personal usuario en lo que a su ámbito de acción aplique.

3. Definiciones

En lo que a las PSI se refieren, los términos que a continuación se detallan, tendrán los siguientes significados:

3.1. Activos:

Elementos a los cuales se les asigna algún valor, en vista de que su ausencia, degradación, o falla, puede tener efectos adversos en los procesos críticos del Ministerio.

3.2. Administración Superior:

Se denominará Administración Superior, a la más alta jerarquía del Ministerio, incluyendo los tres primeros niveles jerárquicos, es decir Ministro, Viceministros y la Oficialía Mayor-Dirección Ejecutiva de la cartera.

3.3. Administrados:

Se denomina Administrados a los destinatarios de los servicios que brinda el Ministerio de Cultura y Juventud.

3.4. Algoritmo:

Secuencia detallada de acciones dirigidas a la realización de una tarea.

3.5. Amenaza:

Son aquellos peligros latentes que de no abordarse adecuadamente, pueden hacer que se exploten las vulnerabilidades de los sistemas informáticos, tecnológicos y/o de información.

3.6. Análisis de riesgos:

Es una consideración sistemática de:

a) El impacto potencial de una falla de seguridad en los procesos que desarrolla la Institución, teniendo en cuenta las potenciales consecuencias que podría acarrear la pérdida de confidencialidad, integridad y/o disponibilidad de la información y otros recursos críticos;
b) La probabilidad de ocurrencia de tal falla, tomando en consideración las amenazas y vulnerabilidades predominantes y los controles previamente establecidos.

Todo análisis de riesgos debe arrojar resultados reproducibles y comparables.

3.7. Anomalía:

Comportamiento errático, viciado, no autorizado o anormal.

3.8. Amenaza:

Son aquellos peligros latentes que de no abordarse adecuadamente, pueden hacer que se exploten las vulnerabilidades de los sistemas informáticos o de información.

3.9. Bloque de Legalidad:

Comprende el marco legal, contractual, normativo, técnico y estratégico que debe aplicar el Ministerio, según el tema de que se trate.

3.10. Cadena de Custodia de la Evidencia:

Es el proceso por medio del cual se garantiza la integridad de la evidencia, desde el momento en que se recopila, hasta el momento en que se hace valer ante las autoridades.

3.11. Confidencialidad de la información:

Asegurar que la información es únicamente accesible a aquellos autorizados para conocerla.

3.12. Conflictos de intereses

Los conflictos de intereses se presentan en toda situación en que los intereses propios y/o personales, (ya sean directos o indirectos), influyen en la toma de las decisiones, haciendo que dicha motivación infiera en el recto cumplimiento de un deber o una obligación.

3.13. Controles:

Medidas adoptadas por el MCJ (incluyendo Políticas, Normas, Estándares, Procedimientos, Medidas Administrativas, Directrices y Lineamientos) para procurar que sus objetivos institucionales se cumplan y así evitar la ocurrencia de eventos no deseables.

Estos deben seleccionarse tomando en cuenta el costo de su implementación, en relación con los riesgos a reducir y las consecuentes pérdidas que podrían generarse de materializarse un incidente de seguridad.

Se entiende también por control, toda aquella medida o contramedida dirigida a salvaguardar los procesos críticos y los servicios prestados por el MCJ.

3.14. Debido Proceso:

Es aquel proceso que ha sido debidamente aprobado por el Ministerio o que se encuentra vigente por ley, y que debe aplicarse de previo al establecimiento de una sanción.

3.15. Debilidad:

Falta o carencia en materia de seguridad.

3.16. Derecho-habiente:

Persona que posee legítimamente un derecho.

3.17. Disponibilidad de la información:

Asegurar que la información y los recursos asociados a ésta, sean accesibles a aquellos autorizados para conocerla, cuando así se requiera.

3.18. Dueño de la Información:

Es toda aquella persona que tiene poder de decisión sobre la información, ya sea porque le pertenece o porque corresponde al ámbito de su competencia.

3.19. Encripción:

Proceso mediante el cual, por medio de la utilización de algoritmos matemáticos, la información se convierte a un formato no legible.

3.20. Equipo informático ajeno autorizado:

Todo aquel equipo (e.g. computadores personales, computadores portátiles, teléfonos inteligentes, de nueva generación; dispositivos de almacenamiento masivo, tablets, palmtops, entre otros) que no siendo propiedad del Ministerio de Cultura y Juventud, es utilizado bajo previa autorización, en actividades de su interés.

3.21. Evento de seguridad:

Es todo aquel acontecimiento que ha sido identificado en un sistema, servicio o red de datos y que da claros indicios de que se ha violentado la normativa en materia de seguridad. Así también forman parte de los eventos de seguridad, situaciones desconocidas que de no ser atendidas, pueden afectar la seguridad de la información del Ministerio.

3.22. Falla:

Es la incapacidad o capacidad limitada de un sistema, recurso o componente de realizar una determinada función que le ha sido requerida.

3.23. Firewall:

Sistema o mecanismo diseñado para prevenir accesos no autorizados desde y hacia redes privadas.

3.24. Firma Digital:

Medio electrónico que identifica y autentica tanto al remitente de un mensaje, como a los datos en él contenidos, por medio del uso de mecanismos de encripción.

3.25. Funcionario

Persona física que labora para el Ministerio.

3.26. Hardware:

Parte física de un computador o sistema.

3.27. Hash:

Es un valor numérico y/o alfanumérico generado por un algoritmo aplicado a un archivo informático determinado, que cumple una función de seguridad, haciendo imposible la alteración de la información contenida en el archivo, sin que a su vez se altere el valor alfanumérico generado.

3.28. Incidentes de Seguridad:

Cualquier tipo de evento (o grupo de eventos) adverso, inesperado o no deseado, que tenga una alta probabilidad de amenazar, poner en riesgo o comprometer, o que efectivamente comprometa, la seguridad de los sistemas, servicios, la información, las redes y/o los procesos críticos del Ministerio. Entendidos estos eventos adversos como fallos en el sistema; uso no autorizado de cuentas ajenas; uso no autorizado de privilegios del sistema; desfase de páginas web; ejecución de códigos maliciosos; fugas de información; destrucción de datos o daños a los sistemas; fugas de agua; incendios, recalentamiento de equipos; bajas o altas en la tensión eléctrica; entre otros.

3.29. Instalaciones de procesamiento de información:

Todas aquellas instalaciones en donde se maneje y/o procese información propiedad del Ministerio y/o en su custodia, sin importar el formato de la información que está siendo manejada o procesada.

3.30. Instrucciones maliciosas:

Son instrucciones, rutinas o programas creados con el objeto de alterar, modificar o dañar el funcionamiento de un sistema, a fin de corromper, destruir o replicar, una parte o la totalidad de los datos almacenados en él. Muchas veces los efectos de las instrucciones maliciosas pueden llegar incluso hasta dañar los equipos tecnológicos. Ejemplos de instrucciones maliciosas, lo constituyen los virus de código fuente, gusanos, Caballos de Troya, entre otros.

3.31. Integridad de la información:

Salvaguardar la exactitud, fidelidad, veracidad y completitud de la información y de sus métodos de procesamiento. La información es íntegra cuando no ha sido modificada, ni alterada sin legítima autorización.

3.32. Interés Público:

El interés público, será considerado como la expresión de los intereses individuales coincidentes de los Administrados.

3.33. Mesa de Servicios:

Función que le permite al Ministerio centralizar los servicios de soporte técnico, cuyo objeto son recursos esenciales de hardware y software.

3.34. Personal Usuario o usuarios:

Los funcionarios, contratistas, vendedores, consultores, ciudadanos, Administrados, proveedores y/o aliados del MCJ a los que se les ha asignado el uso de Recursos Informáticos o se les ha proporcionado acceso a los sistemas de información.

3.35. Puerta trasera:

Debilidad en materia de seguridad que generalmente es diseñada por quienes crean o mantienen programas o aplicaciones y que les permite ingresar a los sistemas, obviando controles de seguridad.

3.36. Pruebas de penetración controlada y pruebas de seguridad:

Son procesos mediante los cuales se evalúan activamente las medidas de seguridad implementadas en la Institución. Estos procesos generalmente consisten en analizar las debilidades técnicas y de diseño, así como el incumplimiento de las Políticas, Normas, Estándares, Procedimientos, Lineamientos, Medidas y Controles aprobados.

3.37. Recursos Informáticos

Son todos aquellos recursos, sistemas, servicios, aplicaciones y/o medios de comunicación, que son propiedad del Ministerio de Cultura y Juventud y/o que son de su interés directo por ser utilizados para las labores propias de éste o en la ejecución de sus objetivos. Estos comprenden entre otros:

a. Recursos de información: Documentación de sistemas, archivos y bases de datos, manuales técnicos de usuario, material de capacitación, procedimientos operativos y de soporte, disposiciones relativas a sistemas de emergencia para la reposición de información, planes de continuidad, diagramas de red, información archivada.
b. Equipo informático: Activos físicos (equipos reproductores, procesadores, monitores, computadores de todo tipo, tablets, dispositivos electrónicos, equipos de comunicaciones (routers, centrales telefónicas, máquinas de fax, teléfonos de todo tipo, contestadores automáticos, redes y enlaces de comunicaciones), medios magnéticos y ópticos; otros equipos técnicos (suministro de electricidad, sistemas de aire acondicionado), mobiliario;
c. Recursos de software: Software de todo tipo (e.g, de sistemas, de aplicaciones, operativos), herramientas de desarrollo, y demás utilitarios;
d. Servicios: Servicios informáticos y de comunicaciones (correo electrónico, Intranet, Internet, entre otros), utilitarios generales (energía eléctrica, iluminación, aire acondicionado).

3.38. Registro:

Compendio de información.

3.39. Responsable Asignado:

Es en última instancia la persona a quien El Ministerio de Cultura y Juventud ha encargado la responsabilidad del cuido y resguardo de los Recursos Informáticos a su cargo.

3.40. Riesgo:

Probabilidad de que un evento no deseado ocurra, afectando la normalidad o la fluidez de los procesos del Ministerio de Cultura y Juventud.

3.41. Riesgo residual:

Es el riesgo que no ha sido cubierto; es aquel riesgo que permanece.

3.42. Riesgo Residual Aceptado:

Es el riesgo que a pesar que no ha sido cubierto, ha sido aceptado por la Administración Superior, quien ha sopesado sus consecuencias.

3.43. Seguridad de la Información:

Es la conservación de la confidencialidad, integridad y disponibilidad de la información. La seguridad de la información también puede implicar aspectos tales como el aseguramiento de la autenticidad de la información, su no repudio y la asignación específica de responsabilidades en la materia.

3.44. Software:

Conjunto de instrucciones ejecutadas por un computador.

3.45. Tercerización:

Cuando aspectos que son propios o están relacionados con la actividad de Tecnología de la Información (e.g. Procesamiento sistematizado de la información), son encomendados a terceras personas físicas o jurídicas.

3.46. Terceros ajenos al Ministerio:

Comprende todas aquellas personas físicas y/o jurídicas que no laboran directamente para el Ministerio de Cultura y Juventud (incluyendo pero sin limitarse a personas o instituciones a las que se les brinda servicio, proveedores, contratistas, asesores, entre otros).

3.47. Visitante:

Se entenderá por visitante a las distintas áreas del Ministerio, toda aquella persona a quien aun cuando no labora directamente para el área a la que desea ingresar, le ha sido autorizado el acceso a ésta, en virtud de haberse comprobado que lo requiere para la realización de sus labores para con la Institución.

3.48. Vulnerabilidad:

Son debilidades asociadas con los activos del MCJ.

4. Responsabilidad

Las responsabilidades de las áreas o puestos involucrados se definen en el cuerpo mismo de las normas aquí incluidas, según corresponda.

5. Descripción

El Ministerio de Cultura y Juventud se ha encomendado la tarea de buscar la mejora continua en su quehacer diario, poniendo especial énfasis en la eficiencia y eficacia de todos sus procesos. Así, además de proveerse de capital humano altamente calificado, se apoya en la tecnología, para lograr cumplir los objetivos institucionales de una manera segura, expedita y responsable.

Este documento de Políticas de Seguridad de la Información (en adelante también denominadas "PSI") está dirigido principalmente a fomentar una cultura de seguridad de la información basada en un modelo de procesos, que le permita al Ministerio, no sólo sentar las bases para cumplir adecuadamente con los deberes que le son impuestos por la normativa nacional aplicable a la materia, sino también utilizar de los Recursos Informáticos y de Información que le son provistos de la mejor manera posible.

En este orden de ideas de conformidad con el ordenamiento jurídico y las mejores prácticas aplicables a la materia, las PSI están basadas principalmente en el estándar internacional ISO/IEC 27002:2013; en las Normas de Gestión y Control de la Seguridad de la Información de la Contraloría General de la República número N-2-2007-CGDFOE; en las Normas emitidas por el Marco de Referencia Cobit 4.1 y en la Ley General de Control interno (en lo que al Ministerio le resulten aplicables).

6. Fecha de creación, y entrada en vigencia de las políticas.

El presente documento fue creado en Enero de 2014, y se encuentra en plena vigencia desde Febrero 2014.

7. Lista de distribución

Las presentes políticas se distribuirán al Personal Usuario directamente involucrado con su cumplimiento, únicamente en lo que a cada uno corresponda.

8. Referencias a otros documentos y anexos

En la elaboración de las Políticas Integral de Seguridad de la Información, se ha tomado como referencia:

a) El Estándar en materia de Seguridad de la Información ISO/IEC 27002:2013;
b) El Estándar para la implementación de Sistemas de Administración de la Seguridad Informática ISO /IEC 27001:2013;
c) La legislación costarricense aplicable a la materia (incluyendo la Ley General de Control Interno -No. 8292 de 31 de julio de 2002-, y Las Normas Técnicas para la Gestión y Control de las Tecnologías de la Información –No. R-CO-26-2007 del 7 de junio, 2007, entre otras);
d) El marco de referencia COBIT v. 4.1. en lo referente a seguridad de la información;
e) Entrevistas y reuniones con personal clave del Ministerio;
f) Doctrina internacional en la materia:

i) ALLEN (Julia), *CERT guide to System and Network Security Practices*, Addison Wesley, Indiana, USA, 2001.
ii) ALTMARK (Daniel Ricardo) y MOLINA QUIROGA (Eduardo), *Contratos Informáticos: La Etapa Precontractual*, Departamento de Posgrado, Facultad de Derecho, Universidad de Buenos Aires, Argentina, 2002.
iii) BARMAN (Scott), *Writing Information Security Policies*, New Riders, Indiana, USA, 2002.
iv) BERGEL (Salvador Darío), *Informática y responsabilidad civil*, Departamento de Posgrado, Facultad de Derecho, Universidad de Buenos Aires, Argentina, 2002.
v) CASTILLO (Francisco), *El Consentimiento del Derecho Habiente*, Editorial Juritexto, San José, C.R., 1998.
vi) CASTRO BONILLA (Alejandra), *Derechos de Autor y Nuevas Tecnologías*, Editorial EUNED, San José, C.R., 2006.
vii) CHINCHILLA (Rosaura), *Ley sobre Registro y Examen de Documentos Privados e Intervención de las Comunicaciones*, IJSA, San José, C.R., 2000.
viii) DAUGHTY (Ken), *Business Continuity Planning*, Auerbach, 2001.
ix) FERNANDEZ LOPEZ (Juan Manuel), *El Derecho a la Privacidad y su frontera con los demás derechos humanos*, Departamento de Posgrado, Facultad de Derecho, Universidad de Buenos Aires, Argentina, 2002.
x) GODERRE (David), *Fraud Detection*, Global Audit Publications, Canada, 1999.
xi) HAMID ABDUL (Rafidah), *the importance of setting up an information management committee*, NISER Web site, 2005.
xii) KILLMEYER (Jan), *Information Security Architecture*, Auerbach, 2001.
xiii) LANDOLL (Douglas J.), *the Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, CRC Press, 2005.
xiv) LAMBERTERIE (Isabel), *Contratos Informáticos*, Departamento de Posgrado, Facultad de Derecho, Universidad de Buenos Aires, Argentina, 2002.
xv) PELTIER (Thomas), *Information Security Risk Analysis*, CRC Press, Florida, USA, 2001.
xvi) PINET (Marcelo), *Datos públicos o datos a los que puede acceder el público y protección de datos personales*, Departamento de Posgrado, Facultad de Derecho, Universidad de Buenos Aires, Argentina, 2002.
xvii) SHERWOOD (John), CLARK (Andrew), LYNAS (David), *Enterprise Security Architecture: A Business-Driven Approach*, CMP Books, 2005.
xviii) SHULTZ (Eugene), *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, New Riders, Indiana, USA, 2002.
xix) STAMP (Mark), *Information Security: Principles and Practice*, John Wiley and Sons, New Jersey, 2011.

9. Del papel protagónico de la Administración Superior en la gestión de Seguridad de la Información

El marco legal aplicable a la gestión tecnológica y en especial a la de la Seguridad de la Información, es claro en rescatar la importancia de la definición de responsabilidades, a todo nivel, partiendo desde el jerarca mismo. De manera que cualesquier determinación que se tome en el desarrollo de la gestión de tecnología de la información, deberá permear desde la máxima autoridad de la Institución, hasta quien ejecuta la conducta relacionada.

El apoyo a las PSI deberá partir pues desde la Administración Superior, a quien corresponderá sentar las bases de la estructura de Seguridad de la Información y dotarla de contenido, de modo que ésta pueda ser efectivamente implementada en la Institución.

En este orden de ideas, las altas jerarquías de la Institución han aprobado el presente documento de Políticas, mediante el cual reafirman el hecho de que la información es un activo institucional del más alto valor, tanto así que la continuidad de las operaciones del Ministerio es completamente dependiente de su integridad y disponibilidad. Cada usuario deberá tener presente que en todo intercambio de información que se realice, sea a lo interno como a lo externo de la Institución, la seguridad deberá tutelarse como un elemento fundamental.

En la aplicación y ejecución de las Políticas, el Ministerio tomará todas las medidas que el ordenamiento jurídico ponga a su alcance, a fin de proteger sus Recursos Informáticos, y su información (y/o aquella que se encuentra bajo su custodia), de cualesquier uso, revelación, modificación, destrucción y/o transmisión no autorizada (incluyendo pero sin limitarse tales medidas a aquellas administrativas, laborales, civiles penales, y/o de cualesquier otra naturaleza que estime convenientes, a fin de sancionar a los responsables).

Además de las Políticas aquí incluidas, el MCJ aprobará todos los Estándares, Procedimientos, Lineamientos, Controles, Directrices y otros comunicados formales que devengan necesarios, a fin de fortalecer la seguridad de su información. Reservándose en todo momento el MCJ, su derecho de realizar el monitoreo legal y legítimo de la operación de todos sus sistemas, incluyendo éste revisiones lógicas y físicas a los Recursos Informáticos, según lo permitido por la legislación aplicable.

10. De la coordinación necesaria en la gestión de Seguridad de la Información

La gestión de la Seguridad de la Información requiere del trabajo coordinado de todos los entes que interactúan en/con el Ministerio de Cultura y Juventud.

10.1. Coordinación de la gestión de Seguridad de la Información

La gestión de la Seguridad de la Información es una responsabilidad que será compartida por todos los miembros de la Institución, pero en especial por la Administración Superior. Por consiguiente deberán establecerse a lo interno del Ministerio, equipos de gestión de

Seguridad de la Información, liderados por niveles directivos con suficiente capacidad de decisión. Estos equipos de gestión serán quienes coordinen la implementación efectiva de las Políticas, los Estándares, Procedimientos, Lineamientos y controles de Seguridad de la Información en toda la Institución, y aseguren que las acciones que se emprendan en materia de seguridad de la información, sean consecuentes con dicha normativa institucional.

11. De las responsabilidades generales de los distintos actores en la Infraestructura de Seguridad del Ministerio

Además de todas las responsabilidades específicas que puedan surgir de las distintas normas que regulan la materia, existen responsabilidades de carácter general, aplicables a los usuarios, según lo establecido por esta sección.

11.1. Responsabilidades generales de los usuarios en materia de seguridad de la información

La seguridad de la información es deber de todos los funcionarios, contratistas, vendedores, proveedores, consultores y/o aliados institucionales, que en función de su relación para con el Ministerio de Cultura y Juventud, tengan acceso a los recursos y sistemas informáticos, así como a las instalaciones físicas donde éstos se encuentran. Es obligación de todos y cada uno de ellos, el cumplimiento estricto y efectivo de las disposiciones que en materia de seguridad de la información, sean debidamente aprobadas por el Ministerio.

11.2. Responsabilidades de las Jefaturas

Los diferentes puestos con personal a cargo del Ministerio de Cultura y Juventud están en la obligación inexcusable de conocer, aplicar y asignar responsabilidades en materia de seguridad de la información, según corresponda.

A fin de poder exigir válidamente las responsabilidades estipuladas por el Ministerio en materia de seguridad de la información, las Jefaturas de la Institución deberán asegurarse de:

a) Proveer los mecanismos necesarios para crear conciencia en los usuarios sobre el papel que les corresponde en la infraestructura de seguridad;
b) Propiciar la suscripción de documentos legales que apoyen la implementación efectiva de las Políticas, Estándares, Procedimientos, Lineamientos y otros comunicados oficiales de Seguridad de la Información establecidos por el Ministerio; y
c) Asesorarse legalmente de previo a la imposición de sanciones, a fin de asegurar en todo momento, la aplicación del debido proceso.

11.3. Constitución de la Comisión de Seguridad de la Información

La Administración Superior deberá constituir una comisión de alto nivel gerencial representativa de toda la organización, cuyos miembros tendrán suficiente capacidad de decisión. Esta Comisión, será la principal encargada de promover la seguridad dentro del Ministerio y de gestionar un presupuesto adecuado para tales efectos.

La Comisión de Seguridad de la Información será de conformación multidisciplinaria, a fin de garantizar una visión integral de la seguridad de la información.

11.4. Conformación de la Comisión de Seguridad de la Información

La Comisión de Seguridad de la Información normalmente estará integrada por:

a) Jefe(a) de la Oficina de Gestión Institucional de Recursos Humanos;
b) Jefe(a) del Departamento Administrativo Financiero;
c) Jefe(a) de la Asesoría Jurídica;
d) Jefe(a) del Departamento de Informática; y
e) Representante de la Administración Superior.

Sin embargo, el Ministerio podrá conformar la Comisión con más personas de estimarlo así necesario, a fin de que se encuentren debidamente representados todas las áreas de la organización y/o de tratar temas específicos en que se requiera de invitados especiales.

11.5. Principales responsabilidades de la Comisión de Seguridad de la Información

Las principales responsabilidades de la Comisión de Seguridad de la Información son[1]:

a) Formular, aprobar y evaluar una estrategia integral de seguridad de la información, que no sólo responda a los objetivos estratégicos institucionales, sino que también ayude a hacer más efectivos los procesos críticos que se desarrollan;
b) Identificar y proponer claramente los objetivos del Ministerio en materia de seguridad de la información, que sean consistentes con los objetivos institucionales;
c) Velar porque los objetivos identificados en materia de seguridad de la información, se integren como parte esencial en todos los procesos críticos del Ministerio;
d) Detallar claramente y delimitar las responsabilidades a ser asignadas para la protección de cada uno de los Recursos Informáticos y de información, así como las responsabilidades a asignarse en la implementación de procesos de seguridad;
e) Definir las responsabilidades específicas para cada uno de los procesos de seguridad y recursos físicos y de información, así como la planeación de la continuidad de los procesos;

[1] KILLMEYER (Jan), *Information Security Architecture*, Auerbach, 2005; HAMID ABDUL (Rafidah), *the importance of setting up an information management committee*, NISER Web site, 2005.

f) Aprobar y evaluar los procesos de seguridad que se emprendan;
g) Aprobar y evaluar las Políticas, los Estándares, Procedimientos, Lineamientos y otros comunicados oficiales en materia de Seguridad de la Información y evaluar también la efectividad en su implementación;
h) Establecer lineamientos sobre la interpretación formal de las Políticas y Políticas de Seguridad de la Información;
i) Proponer cómo se van a manejar las violaciones o quebrantos a la normativa aprobada en materia de seguridad de la información;
j) Proponer y promover las metodologías y procesos a utilizar en materia de seguridad de la información (e.g. metodologías para la valoración de riesgos; para la clasificación de la información, entre otras);
k) Proponer, recomendar y evaluar cambios en/a la normativa de Seguridad de la Información, aprobada por el Ministerio;
l) Aprobar y evaluar cambios de la normativa interna en materia de Seguridad de la Información; cuando se estime conveniente, o en virtud de cambios a lo interno de la Institución, cambios en la legislación aplicable a ésta; cambios importantes en la plataforma tecnológica; problemas en la implementación de los controles aprobados, entre otras razones;
m) Evaluar y coordinar la implementación de controles específicos en materia de seguridad de la información;
n) Asegurarse que la implementación coordinada de los controles de seguridad de la información aprobados, se de en toda la organización;
o) Identificar la necesidad de recurrir a consultoría experta en materia de seguridad de la información, coordinar la aplicación del consejo o guía recibido y analizar los resultados;
p) Establecer requerimientos para la capacitación en Seguridad de la Información, a fin de asegurar el uso adecuado de los recursos tecnológicos;
q) Revisar, promover y aprobar procesos de concientización en materia de Seguridad de la Información;
r) Idear y establecer mecanismos de cooperación para la difusión de la normativa de Seguridad de la Información;
s) Evaluar impactos producidos a raíz de cambios organizacionales que incidan en la Seguridad de la Información;
t) Revisar y evaluar a un alto nivel los incidentes de seguridad, así como y evaluar y aprobar las medidas correctivas instauradas;
u) Evaluar cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes;
v) Definir los mecanismos de administración del flujo de información sensible entre el Ministerio y terceros;
w) Tomar decisiones en materia de Seguridad de la Información, al más alto nivel;
x) Respaldar y gestionar el contenido económico presupuestario las iniciativas en materia de Seguridad de la Información;
y) Obtener el compromiso de apoyo de todas las áreas a las iniciativas de seguridad aprobadas; y
z) Conocer los resultados de la organización de la seguridad.

La Administración Superior será la encargada de definir los límites de las potestades de la Comisión de Seguridad de la Información, así como de asignarle nuevas responsabilidades, de acuerdo a las necesidades específicas del Ministerio.

12. De las responsabilidades específicas de los distintos actores en la Infraestructura de Seguridad del Ministerio

En este aparte se detallan algunas de las responsabilidades específicas aplicables a los distintos involucrados dentro del proceso de gestión de Seguridad de la Información del Ministerio de Cultura y Juventud.

12.1. Rol y responsabilidades del Jefe del Departamento de Informática

La misión del Jefe de la Dirección de Informática es la de dar visión tecnológica y liderazgo para el desarrollo e implementación de las iniciativas de tecnologías de la información. Sus responsabilidades básicas en materia de Seguridad de la Información son:

a) Alinear las Políticas de Seguridad y las estrategias en materia de seguridad, a las objetivos estratégicos del Ministerio de Cultura y Juventud;
b) Vigilar las operaciones de la infraestructura de seguridad y tomar las decisiones con respecto al presupuesto a asignarle a ésta;
c) Establecer y aprobar relaciones y/o alianzas con proveedores clave y consultores en materia de Seguridad de la Información;
d) Establecer los lineamientos para la capacitación en Seguridad de la Información, a fin de asegurar el uso adecuado de los recursos tecnológicos.

12.2. Rol y responsabilidades de las jefaturas de Área

Las jefaturas de área tienen en el ámbito de las Tecnologías de la Información, el deber de vigilar el desarrollo apropiado de todos los sistemas de información, que apoyen directa o indirectamente las funciones críticas que desarrolla el Ministerio de Cultura y Juventud. A fin de cumplir con esta responsabilidad, deberán mantener un nivel de capacitación suficiente en la materia y en caso de no contar con éste, deberán hacerlo saber a los responsables, a fin de solventar la situación.

El nivel de protección a la información que se aplique en todas las áreas del Ministerio, debe ser muy similar.

Las responsabilidades específicas de las jefaturas de Área, en lo que concierne a su ámbito de acción, incluyen:

a) Mantenerse actualizados y capacitados en materia de Seguridad de la Información;
b) Determinar y mantener adecuados controles internos para asegurar que los activos informáticos en su área son suficientemente protegidos;

c) Apoyar los proyectos promovidos por el Ministerio en materia de Seguridad de la información;
d) Velar porque se cumpla lo establecido en las Políticas, en los Procedimientos, Estándares, Lineamientos y en otros comunicados oficiales del Ministerio en materia de Seguridad de la Información;
e) Administrar adecuadamente los riesgos de tecnología de la información;
f) Apoyar conjuntamente con el Encargado de Seguridad de la Información, la creación y desarrollo de la infraestructura de seguridad.
g) Promover y apoyar la realización de evaluaciones de Seguridad de la Información en las oficinas bajo su responsabilidad.

12.3. Rol y responsabilidades del Encargado de Seguridad de la Información

El Encargado de Seguridad de la Información tiene la responsabilidad global de coordinar todos los esfuerzos en la materia.

Las responsabilidades del Encargado de Seguridad incluyen:

a) Mantener comunicación constante con todas las distintas áreas del Ministerio respecto de los riesgos y controles relacionados con el ambiente de los sistemas de operaciones;
b) Recomendar controles de autenticación y acceso de usuarios;
c) Recomendar procesos y metodologías a implementar en materia de Seguridad de la Información;
d) Identificar cambios que puedan comprometer tanto la Seguridad de la Información, como los Recursos Informáticos;
e) Velar porque las Políticas, los Estándares, Procedimientos, Lineamientos y otros comunicados oficiales aprobados por el Ministerio en materia de Seguridad de la Información, sean periódicamente revisados y actualizados y proponer y gestionar cambios
f) Evaluar vulnerabilidades, violaciones, transgresiones e incidentes en materia de seguridad, a fin de asegurar la implementación de controles apropiados;
g) Gestionar las acciones necesarias para que haya una verdadera coordinación institucional en materia de Seguridad de la Información;
h) Guiarse por las mejores prácticas en materia de Seguridad de la Información;
i) Mantener contacto con los proveedores del Ministerio y sitios especializados de seguridad, para lograr una actualización constante en temas de Seguridad de la Información;
j) Gestionar junto con la Oficina de Gestión Institucional de Recursos Humanos los programas de concientización en materia de Seguridad de la Información;
k) Desarrollar, revisar y recomendar las Políticas, los Estándares, Procedimientos y Lineamientos a ser instaurados en el Ministerio.
l) Gestionar programas que impulsen el cumplimiento de las Políticas, los Estándares, Procedimientos, Lineamientos y otros comunicados oficiales aprobados por el Ministerio;
m) Asegurarse que el programa de seguridad como un todo sea efectivamente implementado y actualizado de acorde a los cambios en los ambientes de operaciones y de procesamiento;

n) Comunicar a las distintas áreas y oficinas del Ministerio, las estrategias de control de riesgos que se están implementando, así como para obtener la retroalimentación de éstas en cuanto a sus preocupaciones al respecto.
o) Velar porque los procesos operativos de sistemas resguarden la Seguridad de la Información;
p) Proponer la infraestructura de seguridad y gestionar y abogar por los procesos de implementación;
q) Analizar y proponer soluciones a los problemas de seguridad y de continuidad de las operaciones y servicios críticos del Ministerio; e
r) Identificar los riesgos de cada área del Ministerio y gestionar que se implementen controles para minimizar dichos riesgos.

En un principio el Encargado de Seguridad ejercerá labores eminentemente ejecutivas, debiendo empezar por proponer una infraestructura de seguridad adecuada a las necesidades del Ministerio, misma que requerirá aprobación de la Comisión de Seguridad.

Una vez ya instaurada la infraestructura de seguridad, corresponderá al Encargado de Seguridad dedicarse a las labores de implementación, revisión, evaluación y modificación de las Políticas, los Estándares, Procedimientos, Lineamientos y otras directrices en materia de Seguridad de la Información emanadas del Ministerio de Cultura y Juventud, como respuesta a los procesos de cambio tecnológico y a las valoraciones de riesgo que identifiquen nuevas vulnerabilidades en equipos y sistemas del Ministerio

12.4. Rol y responsabilidades de los Coordinadores de Seguridad

Por cada Dirección, área, y/o unidad funcional independiente deberá nombrarse un Coordinador de Seguridad, a fin de establecer en éstas, las Políticas, los Estándares, Procedimientos, Lineamientos y/o transmitir comunicados oficiales en materia de seguridad de la información. La principal responsabilidad de los Coordinadores de Seguridad será asegurar que en su ámbito de acción, el Personal Usuario cumpla con las normas que en materia de Seguridad de la Información, le apliquen.

Las responsabilidades de los Coordinadores de Seguridad incluyen:

a) Velar porque todos los usuarios comprendidos dentro de su área de acción, firmen los documentos de apoyo legal a la implementación de la Seguridad de la Información;
b) Velar porque se lleven a cabo procesos formales de autorización de accesos a los usuarios, por cada unidad institucional, oficina o departamento a cargo;
c) Vigilar que en razón de la suspensión, despido, vacaciones o cualesquier otro motivo de ausencia de un usuario (funcionario, consultor, proveedor, contratista o aliado institucional) dentro de su unidad institucional, oficina o departamento a cargo, se valore y aplique cualquier modificación o eliminación de los derechos de acceso a los sistemas y recursos del Ministerio, que se estime conveniente;
d) Promover, propiciar, impulsar y conducir, dentro de su unidad institucional, oficina o departamento a cargo, la concientización en materia de Seguridad de la Información;

e) Participar activamente en las actividades y proyectos que promueva el Encargado de Seguridad de la Información; y
f) Coordinar, con el Departamento de Informática, todo lo relacionado con la Seguridad de la Información de su unidad, oficina o departamento a cargo.

12.5. Rol y responsabilidades de las Jefaturas

Para efectos de las PSI, las Jefaturas son aquellos funcionarios responsables directos de cada una de las diferentes unidades institucionales u oficinas del Ministerio. Las Jefaturas tendrán, entre otras, la responsabilidad de:

a) Velar porque los objetivos que en materia de seguridad hayan sido aprobados, sean integrados e implementados como parte fundamental, en los procesos a su cargo;
b) Asegurar en su área de acción, que el Personal Usuario cumpla con las Políticas, los Estándares, Procedimientos y Lineamientos de Seguridad de la Información aprobados por el Ministerio de Cultura y Juventud;
c) Clasificar la información propietaria de su departamento;
d) Autorizar los accesos a la información propietaria de su área, con base en las necesidades específicas de información de cada usuario;
e) Gestionar que en razón de la suspensión, despido, vacaciones o cualesquier otro motivo de ausencia de un usuario (funcionario, consultor, proveedor, contratista o aliado institucional) dentro de su oficina se valore y aplique cualquier modificación o eliminación de sus derechos de acceso a los sistemas y recursos del Ministerio, que se estime conveniente;
f) En caso de suspensión o terminación de una relación contractual o laboral, asegurarse que le sean devueltos al Ministerio, los Recursos Informáticos y la información suministrados en virtud de dicha relación;
g) Motivar, impulsar y conducir, dentro de su oficina, la concientización respecto de la Seguridad de la Información;
h) Asegurar que todos los usuarios comprendidos dentro de su oficina, suscriban debidamente los documentos de apoyo legal a la implementación de la Seguridad de la Información; y
i) Apoyar las labores del Coordinador de Seguridad.

12.6. Rol y responsabilidades de la Oficina de Gestión Institucional de Recursos Humanos

La Oficina de Gestión Institucional de Recursos Humanos es responsable por:

a) Llevar a cabo la contratación, terminación y la aplicación de prácticas disciplinarias, a lo interno de la Institución, con base en lo estipulado en la normativa interna del Ministerio y en la legislación costarricense;
b) Coordinar con las Jefaturas del Ministerio, la entrega en tiempo de información precisa a los administradores de los Recursos Informáticos y de sistemas, respecto de la terminación laboral y/o traslado de usuarios, a fin de que procedan a revocar o modificar los derechos de acceso de dichos usuarios, a los sistemas del Ministerio;

c) Integrar dentro del proceso de inducción el tema de la Seguridad de la Información, de manera que el nuevo personal contratado conozca la importancia que tiene la Seguridad de la Información para el Ministerio;
d) Poner a disposición de los usuarios de recién ingreso las Políticas, los Estándares, Procedimientos, Lineamientos y otros comunicados oficiales formalmente aprobados por el Ministerio en materia de Seguridad de la Información, que correspondan al puesto a desempeñar; y
e) Asegurar que el proceso de contratación incluya la suscripción de documentos legales de apoyo a la implementación y resguardo de la Seguridad de la Información en el Ministerio.

12.7. Rol y responsabilidades de la Asesoría Jurídica

Deberá haber un representante de la Asesoría Jurídica dentro de la Comisión de Seguridad de la Información. Son responsabilidades de la Asesoría Jurídica:

a) Dar carácter de exigibilidad, conforme a la normativa interna del Ministerio y a la normativa nacional que le es aplicable, a las Políticas, los Estándares, Procedimientos y Lineamientos de Seguridad aprobados por el Ministerio;
b) Velar porque cada Norma, Estándar, Procedimiento y Lineamiento de Seguridad a aprobar por el Ministerio, sea conforme a derecho;
c) Mantenerse constantemente actualizado en materia de propiedad intelectual, procesos de encripción; firma y certificados digitales; documentos digitales; protección de datos y en general en cualesquier desarrollo del Derecho Informático especialmente en Costa Rica, para así proponer cambios y modificaciones a las Políticas, los Estándares, Procedimientos y Lineamientos de Seguridad y evitar que el Ministerio incurra en violaciones a derechos protegidos por el ordenamiento, al momento de instaurar controles de seguridad o de adquirir y/o aplicar nuevas tecnologías;
d) Asesorar sobre las consecuencias legales de los controles que en materia de seguridad se instauran en el Ministerio;
e) Tener amplios conocimientos de los principios de derecho penal, que aplican en relación con el uso ilegítimo de los recursos y sistemas informáticos y de las nuevas formas de delincuencia informática;
f) Conocer y asesorar sobre las implicaciones que conlleva la creación; adquisición, el uso, la transmisión y la protección del software, aplicaciones, bases de datos y programas de cómputo;
g) Revisar y aprobar cualesquier documento legal que haya de suscribirse en apoyo a la implementación de las Políticas, los Estándares, Procedimientos y Lineamientos de Seguridad del Ministerio;
h) Asesorar sobre los mecanismos legalmente aceptados de solicitar al Personal Usuario, la suscripción de los documentos legales de apoyo a la implementación de las Políticas, los Estándares Procedimientos y Lineamientos de Seguridad del Ministerio;
i) Asesorar sobre las medidas legales a tomar en virtud de la negativa de un funcionario a suscribir los documentos legales de apoyo a la implementación de las

Políticas, los Estándares, Procedimientos y Lineamientos de Seguridad del Ministerio;

j) Asesorar sobre el manejo apropiado de la confidencialidad de la información del Ministerio, de los Administrados y/o en su custodia; así como sobre la manera de manejar la información personal de los funcionarios de la Institución;
k) Asesorar en asuntos relacionados con quebrantos en la confidencialidad de la información; destrucción de información; archivos y/o programas;
l) Asesorar en cuanto a los procedimientos disciplinarios y/o sancionatorios aplicables, en caso de quebranto o violación de las Políticas, los Estándares, Procedimientos y Lineamientos de Seguridad del Ministerio;
m) Asesorar en los aspectos legales referentes a la recolección, validez y eficacia de las evidencias en materia de Seguridad de la Información (cómputo forense); y
n) Asistir en el desarrollo de los programas de concientización en materia de Seguridad de la Información.

12.8. Mesa de Servicios

El Ministerio de Cultura y Juventud deberá implementar un sistema de Mesa de Servicios que le permita centralizar y agilizar los servicios de soporte técnico, (cuyo objeto son recursos esenciales de software y hardware), a fin de prestar un servicio más eficiente y apoyar a su vez, la gestión en seguridad de la información.

Los servicios de la Mesa de Servicios podrán ser utilizados para:

a) Llevar cuenta de las solicitudes de servicio y el estado de los procesos de soporte que aún no han sido solventados;
b) Llevar cuenta de las áreas del Ministerio con mayores incidencia de problemas;
c) Llevar a cabo inventarios de software y hardware; bitácoras de administración; retiro; adquisición; instalación; movimientos; adiciones; cambios; planeación y diseño; mantenimiento preventivo y correctivo; evaluación de productos; soporte a aplicaciones; integración de sistemas y actualizaciones de programas, entre otros.

12.9. Rol y responsabilidades de la Auditoría Interna

En estricta concordancia con la Ley General de Control Interno y en ejecución de la función asesora de la Auditoria Interna hacia la Administración Superior, ésta debe comprobar en forma oportuna, el estado de aplicación de las Políticas, los Estándares, Procedimientos, Lineamientos y otros comunicados oficiales en materia de seguridad de la información, formalmente aprobados por el Ministerio.

En caso de que se detecten desviaciones, irregularidades e incumplimientos, éstos deberán reportarse por los canales seguros debidamente aprobados por la Institución.

13. Asesoría especializada en materia de Seguridad de la Información

Dado que en la gestión de Seguridad de la Información, puede devenir necesario contar con asesoría especializada en la material, esta sección establece los requerimientos básicos a tener en consideración a ese respecto.

13.1. Asesoría de primer nivel en Seguridad de la Información

En caso de ser necesario, el Ministerio deberá contar con asesoría especializada de primer nivel en materia de Seguridad de la Información. Esta asesoría podrá ser provista ya sea por funcionarios internos que cuenten con conocimientos suficientes en la materia, o dependiendo de la complejidad del asunto o la criticidad de las gestiones de seguridad a realizar, dicha asesoría podrá ser externa.

13.2. Necesidad de los asesores de contar con información histórica y de alto nivel

Los asesores deberán contar con toda la información necesaria, para llevar a cabo sus labores de acuerdo a los requerimientos propios de la Institución. La información a brindarse, sobre todo tratándose de asesores externos, deberá enmarcarse dentro de los criterios de confidencialidad de la misma.

13.3. Asistencia oportuna del asesor en virtud de incidentes y transgresiones de seguridad

Deberá requerirse la asesoría del Encargado de Seguridad en cuanto se tenga conocimiento de la ocurrencia de un incidente o transgresión en materia de Seguridad de la Información.

14. Cooperación entre organizaciones

La gestión de Seguridad de la Información puede facilitarse con el apoyo de aliados externos, siempre que se tomen los cuidados y medidas necesarias para hacerlo de manera segura.

14.1. La Seguridad de la Información se facilita con cooperación global

Deberá mantenerse contacto con autoridades policiales o de seguridad, organismos reguladores, grupos de seguridad informática, proveedores de servicios de información y operadores de telecomunicaciones, a fin de garantizar que, en caso de producirse un incidente de seguridad, puedan tomarse las medidas adecuadas y obtenerse asesoramiento con prontitud.

14.2. Instauración de procedimientos de emergencia

Se deberá contar con procedimientos y controles que determinen y especifiquen:

a) cuándo y a qué autoridades o entidades aliadas contactar en caso de la ocurrencia de un incidente de seguridad; y
b) cómo hacerlo.

Aún frente a la ocurrencia de incidentes de seguridad, deben tomarse las precauciones adecuadas para resguardar la Información Confidencial de la Institución y los Administrados, y determinarse de previo, la forma en la que se dará a conocer el evento.

14.3. Grupos de interés en materia de seguridad de la información

La Institución y en especial, los grupos de trabajo encargados de la seguridad de la información, deberán mantener contacto permanente con foros especializados en la materia, a fin de:

a) Aplicar las mejores prácticas en esta área de acción;
b) Asegurarse que los procedimientos y controles aplicados por la Institución en materia de seguridad de la información, sean completos y estén actualizados;
c) Recibir alertas, advertencias y consejos útiles sobre cómo administrar correctamente amenazas y vulnerabilidades;
d) Tener acceso a parches y nuevos avances tecnológicos, en la materia; y
e) Recibir consejería sobre cómo manejar incidentes de seguridad.

Se debe tener muy presente que nunca, bajo ninguna circunstancia, se ha de dilucidar Información Confidencial propiedad de la Institución o en su custodia, en ningún foro abierto. Sólo podrá darse a conocer información a terceros, cuando éstos hayan suscrito los respectivos acuerdos de resguardo de Información Confidencial y sólo cuando ello sea esencial para fortalecer la infraestructura de seguridad del Ministerio.

De previo implementarse los consejos adquiridos por medio de estos foros, habrá de evaluarse su efectividad y seguridad, en ambientes controlados de prueba dispuestos para tales efectos por la Institución.

15. Inclusión de requerimientos de seguridad desde la descripción de puestos

La tutela Seguridad de la Información deberá ser elemento a tomar en cuenta de manera permanente en las relaciones del Ministerio con sus funcionarios. Así las cosas, la inclusión de requerimientos y controles, en este sentido, deberán darse desde el momento mismo en que se determina el perfil de la persona que se requiere para un puesto determinado.

15.1. La Seguridad de la información desde la etapa de selección de personal

Las responsabilidades en materia de seguridad deberán ser determinadas desde la etapa de selección del personal. Estas deberán ser incluidas en los documentos legales que se suscriban con los funcionarios y además, ser monitoreadas durante las actividades que el individuo desempeñe en virtud de su trabajo.

Los candidatos a ocupar vacantes en la Institución, deberán pasar por un estricto proceso de selección, especialmente cuando su trabajo involucre la realización de tareas críticas.

Este control aplicará, aun cuando el puesto en cuestión, haya de ser ocupado por un funcionario subcontratado (dependiente directamente de una tercera empresa).

15.2. Inclusión de la seguridad en las responsabilidades de los puestos de trabajo

Las funciones y responsabilidades en materia de seguridad, deben ser debidamente documentadas. Estas deben incluir las responsabilidades generales por la implementación y el seguimiento de la normativa de seguridad, así como las responsabilidades específicas por la protección de cada uno de los activos, o por la ejecución de procesos o actividades de seguridad específicos.

15.3. La Seguridad de la Información como elemento a considerar en las evaluaciones de los funcionarios

El cumplimiento efectivo de los requerimientos de Seguridad de la Información establecidos por el Ministerio, será debidamente considerado en todas las evaluaciones de desempeño del personal.

15.4. Selección y política de personal

El análisis de los candidatos a vacantes en el MCJ deberá realizarse teniendo presentes los requerimientos legales y normativos aplicables al puesto, la clase de información que se ha de manejar, y los riesgos de seguridad implicados en el proceso de que se trate.

Se deberán llevar a cabo controles de verificación del personal, desde el momento mismo en que se solicita el puesto. Los controles mínimos a implementar son:

a) Solicitar al menos una referencia personal y una profesional;
b) Comprobar la integridad y veracidad de la hoja de vida presentada por el aspirante;
c) Constatar las aptitudes académicas y profesionales alegadas por el aspirante;
d) Verificar la identidad del aspirante; y
e) Analizar desde una perspectiva global, si el aspirante es la persona idónea para desempeñar el puesto que pretende.

A la información que se recopile del aspirante se le dará el trato de Información Confidencial y ésta sólo deberá ser utilizada única y exclusivamente para los efectos para los que fue recolectada.

Un proceso de selección similar deberá llevarse a cabo con contratistas y personal temporal.

Cuando el personal sea provisto a través de una Bolsa de Empleo, el contrato celebrado entre la Bolsa y el Ministerio deberá especificar claramente las responsabilidades de ésta por la selección.

15.5. Supervisión

Las jefaturas deberán evaluar e indicar los mecanismos de supervisión requerida, para aquel personal nuevo e inexperto a quien se le ha autorizado acceder a sistemas sensibles. El trabajo de todo el personal deberá estar sujeto a revisión periódica y a procedimientos de aprobación por parte de un miembro del personal con mayor jerarquía.

15.6. Términos y condiciones de la contratación

Los términos y condiciones de los contratos de trabajo que se suscriban, deberán establecer la responsabilidad del funcionario por la Seguridad de la Información. Cuando corresponda, estas responsabilidades se extenderán con posterioridad a la finalización de la relación laboral, lo cual deberá quedar debidamente plasmado en los contratos de trabajo.

Se deberá especificar a la vez en estos contratos, que el Ministerio tomará todas las acciones que le son permitidas por el ordenamiento jurídico, a fin de exigir las responsabilidades administrativas, laborales, civiles y/o penales que correspondan, para quienes transgredan las disposiciones en materia de Seguridad de la Información establecidas por el Ministerio.

Las responsabilidades y derechos legales del funcionario en materia de propiedad intelectual y/o protección de sus datos personales, deberán quedar también plasmadas en los contratos de trabajo.

15.7. Del cambio de responsabilidades y la asignación o eliminación de privilegios

Cuando haya de darse un cambio importante de funciones en algún trabajador, que implique a la vez cambio en sus responsabilidades en materia de Seguridad de la

Información o cambio en el perfil de usuario que le fuera asignado previamente, se deberán tomar consideraciones en cuanto a la asignación de nuevos privilegios, así como la eliminación de otros, según ello devenga necesario.

15.8. Inclusión del requerimiento de Confidencialidad de la Información en documentos legales a suscribir

A los usuarios (e.g. funcionarios- temporales y permanentes-, contratistas, consultores, proveedores, aliados) se les requerirá la suscripción de documentos legales, en los que se incluirá la necesidad de protección de la información, durante la vigencia de la relación contractual con la Institución y después de su desvinculación de la misma. Todo ello en estricta conformidad con el ordenamiento jurídico.

De haber cambios en los términos y condiciones de las funciones que desarrollan los usuarios para con la Institución, que impliquen a su vez modificación en sus obligaciones de confidencialidad, ello se hará constar en los documentos legales respectivos.

15.9. Idoneidad para el desarrollo de las labores previstas

Todos los funcionarios así como los aspirantes a puestos dentro de la Institución, sin excepción, tendrán la obligación de comunicar a su superior inmediato, cualesquier tipo de cambios en su situación que le reporten la pérdida de idoneidad para el desempeño de las labores para las cuales fue contratada o se encuentra en proceso de contratación.

La omisión del funcionario del Ministerio en hacer dicha comunicación, dará lugar a la aplicación de las sanciones disciplinarias, incluyendo la terminación del contrato laboral, cuando así corresponda.

16. Formación y capacitación en materia de Seguridad de la Información

La efectiva aplicación de la normativa en materia de Seguridad de la Información, sólo se logra si los diferentes actores reciben la capacitación adecuada para conocerla y comprenderla y si a lo interno de la Institución, se le da la divulgación propicia.

16.1. Responsabilidades en el ámbito de capacitación y divulgación en materia de seguridad de la información

La aplicación práctica de la normativa en materia de seguridad dependerá en gran medida de que reciba una adecuada divulgación a lo interno de la Institución, a fin de que cada usuario entienda con claridad, cuáles son las responsabilidades que le corresponde desarrollar

Será responsabilidad de la Administración Superior garantizar que se brinde capacitación (cuando así corresponda) al Personal Usuario en relación con las Políticas, los Estándares, Procedimientos, Lineamientos y demás directrices en materia de Seguridad de la Información, aprobadas por El Ministerio de Cultura y Juventud.

Por su parte, la Oficina de Gestión Institucional de Recursos Humanos con el apoyo de Departamento de Informática y del Encargado de Seguridad, serán quienes que se encarguen de idear e implementar el plan de capacitación y divulgación respectivo, a fin de asegurar que efectivamente la normativa se dé a conocer a quien corresponda.

La respectiva capacitación deberá ser completa, veraz y oportuna y deberá brindarse incluso antes de que al usuario se le otorguen derechos de acceso a los Recursos Informáticos de la Institución.

Tanto el proceso de capacitación como el de divulgación de la normativa en materia de Seguridad de la Información deberán obedecer a los criterios de resguardo de la información confidencial y/o sensitiva del Ministerio y/o en su custodia, por ende, no deberá darse a conocer más información que aquella que cada grupo de usuarios necesita para cumplir sus objetivos para con la Institución.
Ningún usuario, podrá dar a conocer información alguna sobre la normativa en materia de seguridad aprobada por el Ministerio de Cultura y Juventud, sin contar previamente con autorización formal para hacerlo.

16.2. Disponibilidad para capacitarse en materia de Seguridad de la Información

Es obligación de todo funcionario recibir la capacitación en Seguridad de la Información que El Ministerio de Cultura y Juventud brinde, por ende, cuando se programen actividades de esta índole, el trabajador deberá hacer las previsiones necesarias para atenderlas.

17. De la necesidad de contar con documentos legales de apoyo a la normativa en materia de Seguridad de la Información

Para poder dotar de verdadero carácter de exigibilidad a la normativa en materia de Seguridad de la Información aprobada por el Ministerio, además de fomentar la capacitación y divulgación de las normas correspondientes, deberán establecerse todos los presupuestos legales indispensables para apoyar su cumplimiento efectivo. Es importante resaltar que el listado de documentos que se incluye en esta sección, no es exhaustivo, por lo que posteriormente conforme a sus necesidades y especificidades propias, la Institución será quien defina e implemente la plataforma que más convenga a sus intereses.

17.1. De la plataforma legal básica de apoyo a las Políticas de Seguridad

En virtud de la obligación irrefutable del Ministerio y de sus funcionarios de resguardar el interés público y de manejar los recursos del Estado con la mayor diligencia, la Institución debe constituir una plataforma legal que le permita asegurar, optimizar y efectivizar el uso de los Recursos Informáticos, en estricto apego a la legislación aplicable.

Así, previo acceso a sus Recursos Informáticos o en cualquier otro momento en que el Ministerio lo estime conveniente, al usuario le será requerido suscribir los documentos

legales de respaldo a la aplicación de la normativa en materia de seguridad de la información, que la Institución considere necesarios La aplicación de la normativa en materia de seguridad de la información adoptada por el Ministerio, no deberá oponerse a la legislación aplicable, ni violentar derechos protegidos por el ordenamiento jurídico.

Por ende, para apoyar la aplicación de dicha normativa en pleno cumplimiento con lo anterior, el MCJ requerirá de los usuarios, la suscripción de documentos que les esclarezcan su responsabilidad en la materia y además les informen de las potestades de monitoreo legítimo y necesario que habrá de llevar a cabo la Institución con respecto a sus Recursos Informáticos.

En este orden de ideas, se podrá al menos requerir de los usuarios, según las posibilidades de acceso que se les brinda, la suscripción de los siguientes documentos:

a) **Acuerdo de Confidencialidad**: En este documento se comprometen a mantener toda la información de la que tengan conocimiento con ocasión de su relación con el Ministerio, en estricta confidencialidad y a utilizarla únicamente para los efectos que les fue provista y/o facilitada. Este documento es en realidad aclaratorio, ya que la obligación dicha existe por imposición legal;
b) **Recibo de número de cuenta de usuario**: En este documento se hace acuse de recibo del número de cuenta por parte del usuario; se estipula que entiende los efectos para los cuales le ha sido asignada la cuenta y a la vez, se hace responsable de utilizarla únicamente para dichos efectos, en estricto apego a la normativa aplicable;
c) **Conocimiento de las Políticas de Seguridad**: En este documento se hace acuse de recibo de las Políticas de Seguridad Informática aprobadas por el Ministerio; se hace constar que quien las recibe las ha entendido en todos sus extremos y las acepta, comprometiéndose a la vez, a cumplirlas y a regirse por sus términos. Este documento debe necesariamente tener como complemento indispensable, un programa de capacitación que claramente y de manera suficiente explique los contenidos abordados, enfatizando en las obligaciones y responsabilidades que se asumen y en los alcances de las Políticas de Seguridad de la Información;
d) **Adjudicación de responsabilidad por el manejo del software**: En este documento se hace acuse de recibo de software institucional y se estipula la responsabilidad personal del firmante, de utilizar el software de acuerdo a los términos de su licencia y en estricto apego a la normativa aprobada en materia de seguridad de la información y a la legislación aplicable;
e) **Aceptación de revisión y monitoreo de los Recursos Informáticos**: En este documento se acepta expresamente la potestad del Ministerio para la realización de las actividades de revisión y monitoreo de los Recursos Informáticos, dentro de los límites permitidos por el ordenamiento jurídico y se plasma, a la vez, la voluntad consiente del firmante en dicho respecto;
f) **Leyenda de correo electrónico**: En ésta se establece la confidencialidad de la información que se incluye en el mensaje, se limita su utilización a los autorizados a recibirla y a la vez, se procura reducir la responsabilidad del Ministerio, en caso de:

i) Darse una transmisión incompleta, errónea o a destiempo;

ii) Que la información contenida en el mensaje sea interceptada por terceros no autorizados, para conocer de la misma.

Todo documento legal que haya de requerirse de los usuarios, así como el proceso a seguir para su suscripción, deberá haber sido previamente aprobado por la Asesoría Jurídica.

17.2. De la responsabilidad de la Administración Superior de garantizar que se suscriban los documentos legales de apoyo a la normativa en materia de Seguridad de la Información

Será responsabilidad de la Administración Superior, al más alto nivel, asegurarse que todo usuario (sin excepción) a quien se le conceda acceso a los Recursos Informáticos del Ministerio de Cultura y Juventud, suscriba los documentos legales de conformidad, aceptación y deber de cumplir a cabalidad con las normas adoptadas por la Institución, en materia de seguridad de la información.

18. Cumplimiento de la Política de Seguridad de la Información

A fin de propiciar su efectiva aplicación, el Ministerio vigilará de cerca el cumplimiento de su normativa en materia de Seguridad de la Información, según aplique, por parte de los distintos actores con quienes se relaciona (incluyendo pero sin limitarse éstos a funcionarios, contratistas, aliados institucionales, proveedores, entre otros).

18.1. Obligación del personal usuario de cumplir con la normativa en materia de Seguridad de la Información

Acorde con sus funciones, todos los usuarios tendrán la obligación irrefutable de cumplir estrictamente con las normas en materia de Seguridad de la Información que hayan sido formalmente aprobadas por el Ministerio.

El cumplimiento de las normas en materia de seguridad de la información se considera parte fundamental de las obligaciones de todo usuario y por lo tanto, será permanentemente monitoreado a alto nivel.

18.2. Obligación de los Responsables Asignados de los Recursos Informáticos de colaborar con la verificación de cumplimiento de la normativa en materia de seguridad de la información

Los Responsables Asignados de los Recursos Informáticos del Ministerio, estarán en la obligación irrefutable de prestar toda la colaboración que les sea requerida en la verificación del cumplimiento de la normativa en materia de seguridad de la información

18.3. Verificación de cumplimiento de la normativa en materia de seguridad de la información

Será responsabilidad de las Jefaturas del Ministerio, velar porque las personas que trabajan bajo su cargo cumplan estrictamente con la normativa aprobada en materia de seguridad de la información y de la Administración Superior, garantizar su cumplimiento general. Para ello, se deben implementar revisiones periódicas.

Estas revisiones deben ser llevadas a cabo por personeros capacitados especialmente para tal labor y con experiencia en materia de Seguridad de la Información, los cuales deben tener un criterio objetivo e independiente del área en análisis.

Así, debe verificarse el cumplimiento:

a) De los proveedores, contratistas y demás terceros (en lo que a ellos les aplique);
b) De los Responsables Asignados de los Recursos Informáticos;
c) De los usuarios;
d) De los funcionarios (incluyendo Personal del Departamento de Informática),
e) De las Jefaturas, y
f) De la Administración Superior.

Además, debe tomarse cuenta en la verificación del cumplimiento:

a) La retroalimentación, que en materia de seguridad de la información, viertan personeros involucrados con el tema;
b) Los resultados de revisiones independientes llevadas a cabo por auditores o contratistas externos;
c) El resultado de acciones correctivas o preventivas que en materia de seguridad de la información, se hayan implementado;
d) El resultado de revisiones previas de cumplimiento;
e) El comportamiento de los procesos críticos de la Institución, a raíz de la implementación de nuevos controles;
f) Cualquier cambio capaz de alterar el enfoque hacia la seguridad de la Institución, incluyendo cambios en el ambiente organizacional, en los servicios que se prestan; en la disponibilidad de los recursos con que se cuenta; en las condiciones contractuales, legales o regulatorias que le aplican a la Institución; y cambios en la plataforma técnica;
g) La tendencia hacia ciertas amenazas y vulnerabilidades;
h) Incidentes relacionados con la seguridad de la información, acaecidos en la Institución; y
i) Recomendaciones de autoridades relacionadas con la seguridad de la información (e.g. Contraloría General de la República; Ministerio de Ciencia y Tecnología; Ministerio Público; Organismo de Investigación Judicial; Cuerpos de Policía, entre otros).

En caso de que de la revisión se desprenda que efectivamente se han dado incumplimientos, se deben analizar sus causas; las acciones tendientes a evitar que se repitan; y las acciones correctivas a tomar.

18.4. Reporte resultado de la verificación de cumplimiento de la normativa en materia de seguridad de la información

El resultado de la verificación de cumplimiento se plasmará en un reporte que debe contener, como mínimo, las decisiones y acciones que se estime:

a) Podrán mejorar el enfoque de la organización con respecto a la administración de la Seguridad de la Información;
b) Podrán hacer más eficientes los procesos críticos de la Institución, mejorándose a su vez los servicios brindados;
c) Podrán mejorar los controles de seguridad instaurados, así como sus objetivos;
d) Podrán mejorar la asignación de recursos informáticos y responsabilidades en la materia; y
e) Servirán como medidas correctivas, en caso de que la revisión denote que la administración de la seguridad de la información es defectuosa o inadecuada.

Estos reportes serán conocidos por la Comisión de Seguridad y validados por la Administración Superior y de ellos se llevará un registro, con el fin de poder hacer comparaciones y dar seguimiento.

19. De los procesos disciplinarios

En apoyo al cumplimiento de su normativa en materia de Seguridad de la Información, el Ministerio instaurará procesos disciplinarios, ajustados al ordenamiento jurídico, para quienes la violenten.

19.1. De los requerimientos previos a cumplir a fin de exigir válidamente responsabilidades por violación a las normas

A fin de poder exigir válidamente las responsabilidades estipuladas por el Ministerio en materia de Seguridad de la Información, corresponderá a la Jefaturas de la Institución asegurarse de:

a) Proveer los mecanismos necesarios para generar conciencia en los usuarios sobre el papel que les corresponde en la infraestructura de seguridad;
b) Propiciar la suscripción de documentos legales que apoyen la implementación efectiva de las Políticas, Estándares, Procedimientos, Lineamientos y otros comunicados oficiales de Seguridad de la Información establecidos por el Ministerio;
c) Dar a conocer formalmente la existencia de los procedimientos sancionatorios existentes, y

d) Asesorarse legalmente de previo a la imposición de sanciones, a fin de cumplir en todo momento, con la aplicación del debido proceso.

19.2. De la necesidad de instituir procesos disciplinarios ajustados al ordenamiento jurídico

Con el fin de apoyar efectiva la ejecución y aplicación de la normativa en materia de seguridad de la información, el Ministerio instaurará e implementará, en estricto apego al ordenamiento jurídico, procesos disciplinarios que le permitan sancionar y/o perseguir hasta sus últimas consecuencias y a todo nivel, a quienes la violenten (ya sea por acción u omisión).

Dichos procesos disciplinarios, así como los que tengan como objeto, medio o fin los Recursos Informáticos utilizados por/en el MCJ, deberán obedecer, al menos, a los siguientes criterios:

a) Serán resultado de un debido proceso en respeto al derecho de defensa del presunto responsable;
b) Serán proporcionales a la falta cometida;
c) Se establecerán dentro de los límites permitidos por ley;
d) Se establecerán con el fin de disuadir a los demás usuarios de cometer tales faltas;
e) Iniciarse una vez que se haya verificado la existencia de la falta; y
f) Proveer para que en caso de que la falta sea de carácter gravísimo, por su naturaleza o sus efectos, se remueva todo privilegio y derecho de acceso al presunto infractor, a fin de evitar un daño mayor.

Los procesos disciplinarios deberán ser aplicables a todos los grupos de usuarios dentro de la Institución, a fin de fomentar la cultura de seguridad de la información, en el sentido de que la misma es responsabilidad de todos y no sólo de unos pocos.

20. Procedimientos de evaluación, revisión y cambios a las Políticas de Seguridad.

La normativa en materia de Seguridad de la Información aprobada por el Ministerio no puede ser un elemento estático, por el contrario, deberá ser siempre un elemento vivo que se ajuste a los objetivos estratégicos de la Institución y promueva su cumplimiento. Así, el MCJ instaurará procedimientos de evaluación, revisión y cambios, que permitan mantenerla vigente y efectiva.

20.1. De los procedimientos de evaluación, revisión y cambios de las Políticas

Deberán aprobarse e implementarse procedimientos que permitan evaluar, revisar y hacer cambios a las Políticas de Seguridad de la Información aprobadas por el Ministerio de Cultura y Juventud, cada vez que ello sea necesario, a fin de que éstas se mantengan vigentes, adecuadas y efectivas. Dichos procedimientos deberán incluir tanto

evaluaciones y revisiones periódicas, como esporádicas, en las que se analizarán las oportunidades para mejorar los controles elegidos.

Deberán crearse procedimientos que permitan evaluar, revisar y hacer cambios a las Políticas de Seguridad de la Información:

a) Como mínimo cada año (revisión periódica). Estas revisiones periódicas deberán versar, al menos, sobre:

   i. La adecuación de las normas respectivas, a las Políticas específicas aprobadas por el Ministerio;
   ii. La eficacia de las Políticas;
   iii. El costo e impacto de los controles en la eficiencia de los procesos críticos del Ministerio; y
   iv. Los efectos de los cambios en las tecnologías.

b) Cada vez que se incluyan o eliminen elementos, capaces de afectar los parámetros de riesgo, tomados como base para la elección de los controles aprobados por el Ministerio (e.g. cada vez que se den cambios importantes en la infraestructura de seguridad y/o en los Recursos Informáticos; cada vez que se presenten incidentes de seguridad significativos; cada vez que se den cambios estructurales en la organización; cada vez que se detecten nuevas vulnerabilidades previamente no contempladas, entre otros);
c) Cada vez que la legislación o la normativa relacionada, sufra cambios importantes;
d) Cada vez que haya cambios en los estándares internacionales y en las mejores prácticas en materia de Seguridad de la Información;
e) Cada vez que se le impongan a las entidades del Estado obligaciones en materia de seguridad de la información no contempladas previamente;
f) Cada vez que los procedimientos y procesos críticos así lo requieran; y
g) Cada vez que lo estime necesario la Administración Superior.

Quienes hayan sido expresamente designados para tales efectos, deberán implementar estrictamente los procedimientos de evaluación, revisión y cambios de las Políticas, formalmente aprobados por el Ministerio de Cultura y Juventud.

20.2. De la necesidad de tomar en cuenta las verificaciones de cumplimiento en materia de Seguridad de la Información

La evaluación, revisión y cambio a las Políticas, deberá tomar en cuenta la verificación de cumplimiento de la normativa en materia de Seguridad de la Información, a fin de fomentar de manera permanente, el proceso de mejora continua, así como la eficiencia y efectividad de las mismas.

20.3. Disposiciones finales

➢ **Reserva de derechos del Ministerio**

El Ministerio se reserva el derecho de hacer cualquier tipo de modificación a estas políticas sin que ello implique responsabilidad de su parte, incluso sin previo aviso. Asimismo, la Institución s reserva el derecho de ampararse en una plataforma legal de apoyo a sus políticas, que habrán se suscribir los usuarios que pretendan tener acceso a los Recursos Informáticos.

➢ **Fiscalización de cumplimiento**

El Ministerio se abroga el derecho de controlar estrictamente el debido cumplimiento de estas políticas, así como de tomar cualquier acción, de cualesquier naturaleza, sea ésta civil, penal, laboral y/o administrativa que le sea permitida por el ordenamiento jurídico, con el fin de castigar la violación a las mismas, para lo cual deberá respetar el debido proceso.

➢ **Usos ilícitos y/o no permitidos**

El Ministerio facilita sus Recursos Informáticos únicamente para usos permitidos y legales. Por ende, quien haga uso de los mismos para fines ilegales y/o no permitidos, deberá asumir todas y cada una de las consecuencias que de su actuar u omisión deriven.

➢ **Políticas como una guía básica**

Las políticas incluidas en el presente documento pretenden ser una guía básica, no una lista exhaustiva. Por ende, de tener el usuario alguna duda que las Políticas no puedan aclarar, deberá consultarla, según corresponda, ya sea con el Jefe del área a que pertenece; con el supervisor del proyecto de que se trate; y/o con quien dirige el Departamento de Informática.

➢ **Tolerancia**

El que el Ministerio por cualesquier razón decida no tomar acciones en un determinado momento para exigir responsabilidades o sancionar algún comportamiento, no impide que pueda hacerlo en cualquier momento posterior. Deberá tenerse presente que el Ministerio estará siempre en potestad de actuar, según se lo permita el ordenamiento jurídico aplicable.