ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE CULTURA,
RECREACIÓN Y DEPORTE

ALCALDÍA MAYOR DE BOGOTÁ SECRETARIA DE CULTURA, RECREACION Y DEPORTE

Dirección de Gestión Corporativa
Grupo Interno de Sistemas

NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA

Manual de Normas y Políticas de Seguridad de la información V.

2012-2016

BOGOTÁ, NOVIEMBRE DE 2012

SECRETARIA DISTRITAL DE CULTURA, RECREACIÓN Y DEPORTE

NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA

Manual de Normas y Políticas de Seguridad de la información V.1.0

El documento que se presenta como normas y políticas de seguridad pretende ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que **La Secretaria Distrital De Cultura, Recreación y Deporte - SCRD**, previene, protege y maneja los riesgos de seguridad de la información en diversas circunstancias.

El ámbito de aplicación del manual de normas y políticas de seguridad informática, es la infraestructura tecnológica y entorno informático de la red de la SCRD.

El ente que garantizará la ejecución y puesta en marcha de la normativa y políticas de seguridad, estará bajo el cargo del Grupo Interno de Sistemas, siendo el responsable absoluto de la supervisión y cumplimiento; debe designar un Oficial Seguridad de la Información, seleccionado y supervisado por la Gerencia

Alcance: El presente documento describe las políticas y los estándares de seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso de los equipos de cómputo, aplicaciones y servicios informáticos de la SCRD.

Beneficios: Las políticas y estándares de seguridad informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información de la SCRD.

I. INTRODUCCIÓN

En una organización la gestión de seguridad puede tornarse compleja y difícil de realizar, esto no por razones técnicas, sino por razones organizativas. Coordinar todos los esfuerzos encaminados para asegurar un entorno informático institucional, mediante la simple administración del recurso humano y tecnológico, sin un adecuado control que integre los esfuerzos y conocimiento humano con las técnicas depuradas de mecanismos automatizados, tomará en la mayoría de los casos un ambiente inimaginablemente hostil; por ello es necesario emplear mecanismos

reguladores de las funciones y actividades desarrolladas por cada uno de los empleados de la SCRD.

El documento que se presenta como el manual, recopila las normas y políticas de seguridad que se implementarán en la SCRD e integra estos esfuerzos de una manera conjunta. Éste manual pretende ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la institución prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias.

Las normas y políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser normas absolutas; las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad y los procedimientos de control de cambios establecidos por los sistemas de gestión de Calidad de la SCRD.

Toda persona que utilice los servicios que ofrece la red deberá conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

En términos generales, el manual de normas y políticas de seguridad informática engloba los procedimientos más adecuados, tomando como lineamientos principales cuatro criterios que se detallan a continuación:

Seguridad Organizacional: Dentro de este criterio se establece el marco formal de seguridad que debe sustentar la institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, Integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Lógica: Trata de establecer e integrar los mecanismos y procedimientos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

Seguridad Física Asociada a la Información: Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

Seguridad Legal: Integra los requerimientos de seguridad que deben cumplir todos los funcionarios, contratistas y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la SCRD en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

Cada uno de los criterios anteriores sustenta un entorno de administración de suma importancia para la seguridad de la información dentro de la red institucional de la SCRD.

Las políticas fueron creadas según el contexto de aplicación, organizadas por niveles de seguridad y siguiendo un entorno de desarrollo alrededor de la problemática de la institución y previniendo futuras rupturas en la seguridad aplicada sobre los diferentes recursos o activos de la institución.

Los niveles de seguridad han sido organizados constatando un enfoque objetivo de la situación real de la institución, desarrollando cada política con sumo cuidado sobre qué activo proteger, de qué protegerlo, cómo protegerlo y por qué protegerlo. Los mismos se organizan siguiendo el esquema normativo de seguridad ISO 27001 (mejores prácticas de seguridad) y se presentan a continuación.

Nivel de Seguridad Organizacional:

- Seguridad Organizacional
- Políticas de Seguridad
- Excepciones de Responsabilidad
- Clasificación y Control de Activos
- Responsabilidad por los Activos
- Clasificación de la Información
- Seguridad Ligada al Personal
- Capacitación de Usuarios
- Respuestas a Incidentes y Anomalías de Seguridad

Nivel de Seguridad Física:

- Seguridad Física
- Seguridad Física y Ambiental
- Seguridad de los Equipos
- Controles Generales

Nivel de Seguridad Lógico:

- Control de Accesos

- Administración del Acceso de Usuarios
- Seguridad en Acceso de Terceros
- Control de Acceso a la Red
- Control de Acceso a las Aplicaciones
- Monitoreo del Acceso y Uso del Sistema

Nivel de Seguridad Legal:

- Seguridad Legal
- Conformidad con la Legislación
- Cumplimiento de Requisitos Legales
- Revisión de Políticas de Seguridad y Cumplimiento Técnico
- Consideraciones Sobre Auditorias de Sistemas

II. DEFINICIÓN DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA

¿Que son las Normas de Seguridad?

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles formuladas con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional.

¿Que son las Políticas de Seguridad?

Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

¿Cual es la importancia de los Manuales?

Como parte integral de un Sistema de Gestión de Seguridad de la Información (SGSI), un manual de normas y políticas de seguridad, trata de definir; ¿Qué?, ¿Por qué?, ¿De qué? y ¿Cómo? se debe proteger la información. Estos engloban una serie de objetivos, estableciendo los mecanismos necesarios para lograr un nivel de seguridad adecuado a las necesidades establecidas dentro de la institución. Estos documentos tratan

a su vez de ser el medio de interpretación de la seguridad para toda la organización.

III. ORGANIZACIÓN DE LA SEGURIDAD INFORMÁTICA

El sistema de Seguridad de la Información al interior de la SCRD estará conformado por personas que de manera no exclusiva y sin afectar sus labores cotidianas asumirán los siguientes roles:

GERENCIA DE SEGURIDAD: Autoridad de nivel superior que integra el comité de seguridad. Bajo su administración están la aceptación y seguimiento de las políticas y normativa de seguridad en concordancia con las autoridades de nivel superior.

GESTOR DE SEGURIDAD: Persona dotada de conciencia técnica, encargada de velar por la seguridad de la información, coordinar auditorías de seguridad, actualizar documentos de seguridad como políticas, normas; y de llevar, con la ayuda de la unidad de informática, un estricto control referente a los servicios prestados y niveles de seguridad aceptados para tales servicios.

RESPONSABLE DE LOS ACTIVOS: Personal dentro cada una de las diferentes áreas de la institución, que velará por la seguridad y correcto funcionamiento de los activos informáticos, así como de la información procesada en éstos, dentro de sus respectivas áreas o niveles de mando.

IV. MARCO DE DESARROLLO

Para establecer las políticas de seguridad se consideraron los lineamientos generales establecidos mediante el Acuerdo Distrital 057 de 2002 y demás normas dictadas por la Comisión Distrital de Sistemas. En especial, se consideraron las Políticas Generales de Tecnología de Información y Comunicaciones aplicables a las entidades del Distrito Capital.

Se asume, tal y como lo establece la Comisión Distrital de Sistemas, que cada una de las políticas y lineamientos de este manual son de actualización continua y deben ser aplicadas al interior de las dependencias que conforman las entidades distritales responsables de la implementación del SDI, teniendo en cuenta que las tecnologías de información y comunicaciones son medios que permiten la consolidación de una cultura de participación ciudadana en la administración de lo público y un acercamiento de la Administración Distrital a la ciudadanía.

V. METRICA DE RESULTADOS

El logro de los objetivos planteados exige un compromiso real de la entidad y de sus directivos, responsables de implementar los mecanismos de seguimiento y coordinación institucional e interinstitucional que permitan que el SGSI se constituya verdaderamente en un instrumento de gestión eficiente y eficaz para la toma de decisiones por parte de la Administración Distrital.

El éxito se medirá mediante evaluación del grado de implementación de las directrices necesarias para el correcto funcionamiento del sistema de gestión para la seguridad de la información, enmarcando su aplicabilidad en un proceso de desarrollo continuo y actualizable, apegado a los estándares internacionales desarrollados para tal fin.

VI. ALCANCES Y ÁREA DE APLICACIÓN

El ámbito de aplicación del manual de normas y políticas de seguridad informática, es la infraestructura tecnológica y entorno informático de la red institucional de la SCRD.

POLITICAS

1. POLÍTICAS DE SEGURIDAD INFORMÁTICA

1.1. OBJETIVO

Dotar de la información necesaria en el más amplio nivel de detalle a los usuarios, empleados y gerentes de la SCRD, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red institucional, así como la información que es procesada y almacenada en estos.

1.2. SEGURIDAD ORGANIZACIONAL

Todos los usuarios de bienes y servicios informáticos de la SCRD deben firmar un convenio (ANEXO I) en el que acepten las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática.

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

1.2.1. POLÍTICAS DE SEGURIDAD

A. Los servicios de la red institucional son de exclusivo uso operativo, técnicos y para gestiones administrativas relacionados con la actividad

de la SCRD; cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento.

B. La SCRD nombrará un comité de seguridad que hará seguimiento al cumplimiento de la normativa y propiciará el entorno necesario para crear un SGSI, el cual tendrá entre sus funciones:
   - Velar por la seguridad de los activos informáticos
   - Garantizar el cumplimiento de políticas.
   - Aplicar las sanciones en caso de ser necesario.
   - Elaborar de planes de seguridad.
   - Capacitar a los usuarios en temas de seguridad.
   - Gestionar y coordinar esfuerzos para crear un plan de contingencia que dé sustento o solución a problemas de seguridad dentro de la institución.
   - Orientar y guiar a los funcionarios y contratistas en la forma o métodos necesarios para salir avante ante cualquier eventualidad que se presente.
   - Divulgar procedimientos que permitan informar sobre problemas de seguridad a la alta dirección.

C. Todo usuario de la red institucional de la SCRD gozará de privacidad limitada sobre su información o la información que provenga de sus acciones. La SCRD podrá monitorear la actividad para evitar que ésta se vea involucrada en actos ilícitos o contraproducentes para la seguridad de la red institucional, sus servicios o cualquier otra red ajena a la entidad.

D. Los usuarios tendrán el acceso a Internet siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad de informática.

E. Las actividades operativas (operación óptima de los puntos de atención y labores de procesamiento de datos) tienen la primera prioridad, por lo que a cualquier usuario utilizando otro servicio (por ejemplo Internet o "Chat") sin estos fines, se le podrá limitar en tiempo real estos servicios, si así, fuera necesario.

1.2.2. CLASIFICACIÓN Y CONTROL DE ACTIVOS

RESPONSABILIDAD POR LOS ACTIVOS

A. Cada Unidad organizativa o área de trabajo tendrá un responsable por el/los activo/s crítico/s o de mayor importancia para la entidad.
B. La persona responsable de los activos de cada unidad organizativa o área de trabajo, velará por la salvaguarda de los activos físicos

(hardware y medios magnéticos, aire acondicionado, mobiliario.), activos de información (Bases de Datos, Archivos, Documentación de sistemas, Procedimientos Operativos, configuraciones), activos de software (aplicaciones, software de sistemas, herramientas y programas de desarrollo)

C. Los administradores de los sistemas son los responsables de la seguridad de la información almacenada en esos recursos.

D. Con el fin de determinar la propiedad de los activos se establecerá un inventario que contendrá los siguientes campos:
   a. Nombre del Activo: Es un campo que define la manera como se va a reconocer el activo de información en el proceso y la entidad, con un nombre particular y diferenciable.
   b. Descripción del activo: Información adicional que permita identificar de manera única el activo de información o su importancia dentro de la entidad o proceso. Esta información también permite determinar si el activo de información comprende otros activos. Por ejemplo, “Información de procesos disciplinarios” este activo puede contener entre otros: la hoja de vida del procesado, evidencias, información de descargos, etc. Otro ejemplo, “Información de contratos”: este activo puede contener: pliego de requerimientos, preguntas por parte de los licitantes, propuestas, evaluaciones, etc..
   c. Propietario, y
   d. Custodio Técnico.

CLASIFICACIÓN

A. De forma individual, las unidades administrativas que interactúan con la SCRD, son responsables de clasificar de acuerdo al nivel de importancia, la información que en ella se procese. Se tomarán como base los siguientes criterios, como niveles de importancia, para clasificar la información:
   - Pública
   - Interna
   - Restringida
   - Confidencial

B. Los activos de información de mayor importancia para la institución deberán clasificarse por su nivel de exposición o vulnerabilidad.

C. Se define el tipo al cual pertenece el activo. Para este efectos se utilizan los siguientes opciones:

Información: a este tipo de activos corresponden: datos, sistemas de información e información almacenada o procesada física o electrónicamente como por ejemplo: las bases de datos, archivos de

datos, contratos, acuerdos, documentación del sistema, información sobre investigaciones, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro, pruebas de auditoría e información archivada física o electrónicamente.

Software: Dentro de este tipo de activos se encuentran herramientas de ofimática, herramientas de propósito específico, herramientas de desarrollo, utilidades, aplicaciones para acceso a la información. No se incluyen los sistemas de información.

Hardware: Son activos como: Equipos de computación, equipos de comunicaciones, medios removibles, instrumentos particulares para la ejecución del proceso y otros equipos físicos.

Servicios: Servicios de computación y comunicaciones. (ejemplo: Acceso a Internet, páginas de consulta, acceso a la red, etc.), servicios de outsorcing.

1.2.3 SEGURIDAD LIGADA AL PERSONAL

Referente a contratistas:

Se entregará al contratista toda la documentación necesaria para ejercer sus labores dentro de la institución, sólo en el momento en que esté legalizado su contrato laboral. La información procesada, manipulada o almacenada por el contratista es propiedad exclusiva de la SCRD.

CAPACITACIÓN DE USUARIOS

A. Los usuarios de la red institucional serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.
B. Se deben tomar todas las medidas de seguridad necesarias antes de realizar una capacitación a personal ajeno o propio de la institución, siempre y cuando se vea implicada la utilización de los servicios de red o se exponga material de importancia considerable para la institución.

RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD

A. Se realizarán respaldos diarios de la información para los activos de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado mensualmente el cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.

B. El gestor de seguridad deberá elaborar un documento donde explique los pasos que se deberán seguir en situaciones contraproducentes a la seguridad y explicarlo detalladamente en una reunión ante el personal de respuesta a incidentes.
C. Cualquier situación anómala y contraria a la seguridad deberá ser documentada, posterior revisión de los registros o Log de sistemas con el objetivo de verificar la situación y dar una respuesta congruente y acorde al problema, ya sea esta en el ámbito legal o cualquier situación administrativa.

1.2.4 SEGURIDAD LÓGICA

CONTROL DE ACCESOS

A. El Gestor de Seguridad proporcionará toda la documentación referente a formularios, guías, controles, otros, necesaria para agilizar la utilización de los sistemas
B. Cualquier petición de información, servicio o acción proveniente de un determinado usuario o departamento, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la entidad para realizar dicha acción; no dar seguimiento a esta política implica:
   - Negar por completo la ejecución de la acción o servicio.
   - Presentar un Informe completo dirigido al comité de seguridad, el cual será realizado por la persona o el departamento al cual le es solicitado el servicio.
   - Imponer sanciones aplicables por autoridades de nivel superior, previamente discutidas con el comité de seguridad.

ADMINISTRACIÓN DEL ACCESO DE USUARIOS

A. Son usuarios de la red institucional todas aquellas personas que tengan carácter de empleado, contratista u otra vinculación, y utilice los servicios de la red institucional de la SCRD.
B. Se asignará una cuenta de acceso a los sistemas de la intranet a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.
C. Los empleados de carácter no directivo son usuarios limitados, estos tendrán acceso únicamente a los servicios y recursos que su perfil así lo determine; cualquier cambio sobre los servicios a los que estos tengan acceso será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.
D. Se consideran usuarios externos o terceros, cualquier entidad o persona natural que tenga una relación con la institución fuera del ámbito de empleado y siempre que tenga una vinculación con los servicios de la red institucional.

E. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia la entidad y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.
F. No se proporcionará el servicio solicitado por un usuario sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.
G. La asignación de las contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
H. La longitud mínima permisible en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica incluyendo caracteres especiales.
I. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá levantar un reporte al Centro de Atención a Usuarios para que se le proporcione una nueva contraseña y una vez que la reciba, deberá cambiarla en el momento en que acceda nuevamente a la infraestructura tecnológica.
J. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarla inmediatamente.

RESPONSABILIDADES DEL USUARIO

A. El usuario es responsable exclusivo de mantener a salvo su contraseña.
B. El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios.
C. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta sea guardada en un lugar seguro.
D. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Gestor de Seguridad, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.
E. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.
F. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en el
G. Cualquier usuario que encuentre una vulnerabilidad o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo a los administradores del sistema o gestor de seguridad.
H. El uso del servicio de correo electrónico se debe hacer acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional. Todo uso indebido del servicio de correo electrónico será motivo de suspensión temporal o definitiva de la cuenta de correo.

I. El usuario será responsable de la información que sea enviada con su cuenta.
J. El comité de seguridad se reservará el derecho de monitorear las cuentas de usuarios que presenten un comportamiento sospechoso para la seguridad de la red institucional.
K. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software, información de tipo restringido o reproducir información sin conocimiento del autor.

SEGURIDAD EN EL ACCESO DE TERCEROS

A. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las entidades involucradas en el mismo.
B. Todo usuario externo estará facultado a utilizar única y exclusivamente el servicio que le fue asignado y acatar las responsabilidades que devengan de la utilización del mismo.
C. En los servicios accedidos por terceros se acatarán las disposiciones generales de acceso a servicios por el personal interno de la institución, además de los requisitos expuestos en su contrato con la entidad.

CONTROL DE ACCESO A LA RED

A. El acceso a la red interna se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido mediante un mecanismo de autenticación.
B. Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso.
C. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoria de seguridad.
D. Se deberán emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información no autorizada hacia la red interna o desde la red interna hacia el exterior.
E. Los accesos a la red interna o local desde una red externa de la institución o extranet, se harán mediante un mecanismo de autenticación seguro y el trafico entre ambas redes o sistemas será cifrado con una encriptación de al menos 128 bit.
F. Se registrará todo acceso a los dispositivos de red mediante archivos de registro o Log de los dispositivos que provean estos accesos.
G. Se efectuará una revisión de Log de los dispositivos de acceso a la red en un tiempo máximo de 48 horas.

CONTROL DE ACCESO AL SISTEMA OPERATIVO

A. Se deshabilitarán las cuentas creadas por ciertas aplicaciones con privilegios de sistema, (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, etc.) evitando que estas corran sus servicios con privilegios nocivos para la seguridad del sistema.
B. Al terminar una sesión de trabajo en las estaciones o cualquier otro usuario, se evitará dejar encendido el equipo para evitar que pueda proporcionar un entorno de utilización de la estación de trabajo.
C. El acceso a la configuración del sistema operativo de los servidores es únicamente permitido al usuario administrador.
D. Los administradores de servicios tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.
E. Todo servicio provisto o instalado en los servidores correrá o será ejecutado bajo cuentas restrictivas; se evitarán situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

CONTROL DE ACCESO A LAS APLICACIONES

A. Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso específicas para cada usuario del entorno operativo de la aplicación, las prestaciones de la aplicación deben permitir el manejo de log de conexiones..
B. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.
C. Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones de forma aleatoria, sobre distintas fases y antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.
D. Las salidas de información de las aplicaciones en un entorno de red, deberán ser documentadas y especificar la terminal por la que deberá ejecutarse exclusivamente la salida de información.
E. Se deberá llevar un registro, mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

MONITOREO DEL ACCESO Y USO DEL SISTEMA

A. Se registrará y archivará toda actividad procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

B. Los archivos de Log almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.
C. Se efectuará una copia automática de los archivos de Log y se conducirá o enviará hacia otra terminal o servidor, evitando se guarde la copia localmente donde se produce.

1.3. GESTIÓN DE OPERACIONES Y COMUNICACIONES

RESPONSABILIDADES Y PROCEDIMIENTOS OPERATIVOS

A. El personal administrador de algún servicio es el responsable absoluto por mantener en óptimo funcionamiento ese servicio, coordinar esfuerzos con el gestor de seguridad, para fomentar una cultura de administración segura y servicios óptimos.
B. Las configuraciones y puesta en marcha de servicios son reguladas por el departamento de informática y el comité de seguridad.
C. El personal responsable de los servicios llevará archivos de registro de fallas de seguridad del sistema, revisará estos archivos de forma frecuente y en especial después de ocurrida una falla.

PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

A. La unidad de informática, con la dirección de los líderes a través del personal dedicado o asignado en el área de programación o planificación y desarrollo de sistemas, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para la SCRD.
B. La aceptación del software se hará efectiva por la Gerencia de la institución, previo análisis y pruebas efectuadas por los usuarios directos en su parte funcional y en su parte técnica por el personal de informática
C. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado por personal calificado en el área de seguridad.
D. La aceptación y uso de los sistemas no exonera de responsabilidad alguna sobre el gestor de seguridad, para efectuar pruebas o diagnósticos a la seguridad de los mismos.
E. El software diseñado internamente, deberá ser analizado y aprobado por el gestor de seguridad antes de su implementación.
F. Es tarea de programadores el realizar pruebas de validación de entradas, en cuanto a:
   - Valores fuera de rango.
   - Caracteres inválidos, en los campos de datos.
   - Datos incompletos.

- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.
- Procedimientos operativos de validación de errores
- Procedimientos operativos para validación de caracteres.
- Procedimientos operativos para validación de la integridad de los datos.
- Procedimientos operativos para validación e integridad de las salidas.

G. Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.
H. Cualquier prueba sobre los sistemas deberá ser documentada y cualquier documento o archivo que haya sido necesario para su ejecución deberá ser borrado de los dispositivos físicos, mediante tratamiento electrónico.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

A. Se adquirirá y/o utilizará software únicamente de fuentes confiables.
B. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus, antispyware y antispam actualizable y activada la protección en tiempo real.

MANTENIMIENTO

A. El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal de la unidad de informática, o del personal de soporte técnico.
B. El cambio de archivos de sistema, no es permitido sin una justificación aceptable y verificable por el gestor de seguridad.
C. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

A. Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la institución, serán etiquetados de acuerdo con la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.
B. Los medios de almacenamiento con información crítica y las copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.
C. Todo medio de almacenamiento con información crítica será guardado bajo llave en una caja especial, a la cual tendrá acceso únicamente el

gestor de seguridad o la gerencia administrativa; esta caja no debería ser removible. Una segunda copia será resguardada por un tercero, entidad de custodia o afín.

D. Se llevará un control en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

1.4. SEGURIDAD FÍSICA

1.4.1. SEGURIDAD FÍSICA Y AMBIENTAL

SEGURIDAD DE LOS EQUIPOS

A. El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.
B. Los servidores con problemas de hardware, sin importar al grupo al que estos pertenezcan, deberán ser reparados localmente; de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.
C. Los equipos o activos críticos de información y proceso deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el gestor de seguridad y las personas responsables por esos activos, quienes deberán poseer su debida identificación.

CONTROLES GENERALES

A. Las estaciones o terminales de trabajo con procesamientos críticos, no deben de contar con medios de almacenamientos extraíbles que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información. En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.
B. Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.
C. Toda visita a las oficinas de tratamiento de datos críticos e información (unidad de informática, sala de servidores entre otros) deberá ser registrada mediante el formulario de accesos a las salas de procesamiento crítico, para posteriores análisis del mismo.
D. La sala o cuarto de servidores, deberá estar separada de las oficinas administrativas de la unidad de informática o cualquier otra unidad, departamento o sala de recepción del personal, mediante una división recubierta de material aislante o protegido contra el fuego. Esta sala

deberá ser utilizada únicamente por las estaciones prestadoras de servicios y/o dispositivos a fines.

E. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.
F. El suministro de energía eléctrica debe estar debidamente polarizado**.**
G. Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica polarizada a tierra y proveer de un circuito de suministro de energía regulada exclusivo para los equipos de infirmatica, especialmente en los servidores mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.
H. Las instalaciones físicas de procesamiento de información deberán brindar información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.

1.5. SEGURIDAD LEGAL

1.5.1. CONFORMIDAD CON LA LEGISLACIÓN

CUMPLIMIENTO DE REQUISITOS LEGALES

Licenciamiento de Software:

A. La SCRD, se reserva el derecho de respaldo, a cualquier funcionario, ante cualquier asunto legal relacionado con infracciones a las leyes de copyright o piratería de software.
B. Todo el software comercial que utilice la SCRD deberá estar legalmente registrado en los contratos de arrendamiento de software con sus respectivas licencias.
C. La adquisición de software por parte de personal que labore en la institución, no expresa el consentimiento de la institución. La instalación del mismo no garantiza responsabilidad alguna para la entidad, por ende la institución no se hace responsable de las actividades de sus empleados.
D. Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores; la entidad respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores.
E. El software comercial licenciado a la SCRD es propiedad exclusiva de la entidad; la misma se reserva el derecho de reproducción de éste sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

F. En caso de transferencia de software comercial a terceros, se harán las gestiones necesarias para su efecto y se acatarán las medidas de licenciamiento relacionadas con la propiedad intelectual.
G. Las responsabilidades inherentes al licenciamiento de software libre son responsabilidad absoluta de la SCRD.
H. Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y en base a las disposiciones de la respectiva licencia.
I. El software desarrollado internamente por el personal que labora en la institución, es propiedad exclusiva de la SCRD.
J. La adquisición del software libre o comercial deberá ser gestionado con las autoridades competentes y acatando sus disposiciones legales, en ningún momento se obtendrá software de forma fraudulenta.
K. Los contratos con terceros en la gestión o prestación de un servicio, deberán especificar las medidas necesarias de seguridad, nivel de prestación del servicio, y/o el personal involucrado en tal proceso.

REVISIÓN DE POLÍTICAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

A. Toda violación a las políticas de licenciamiento de software será motivo de sanciones aplicables al personal que incurra en la violación.
B. El documento de seguridad será elaborado y actualizado por el gestor de seguridad junto al comité de seguridad; su aprobación y puesta en ejecución será responsabilidad de la gerencia administrativa.
C. Cualquier violación a la seguridad por parte del personal que labora para la entidad así como por terceros que tengan relación o alguna especie de contrato con la institución, se harán acreedores a las sanciones aplicables de ley

CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS

A. Se debe efectuar una auditoria trimestral de seguridad a los sistemas de acceso a la red, enmarcada en pruebas de Ethical hacking y análisis de vulnerabilidad.
B. Toda auditoria a los sistemas estará debidamente aprobada y tendrá la firma de la gerencia.
C. Cualquier acción que amerite la ejecución de una auditoria a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos de la misma, así como razones para su ejecución, personal involucrada en la misma y sistemas implicados.
D. La auditoría no deberá modificar en ningún momento el sistema de archivos de los sistemas implicados; en caso de haber necesidad de modificar algunos, se deberá hacer un respaldo formal del sistema o sus archivos.

E. Las herramientas utilizadas para la auditoria deberán estar separadas de los sistemas de producción y en ningún momento éstas se quedarán al alcance de personal ajeno a la elaboración de la auditoria.

GLOSARIO DE TERMINOS

Activo: Es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios; en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración Remota: Forma de administrar los equipos informáticos o servicios de la SCRD, a través de terminales o equipos remotos, físicamente separados de la institución.

Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Archivo Log: Archivos de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, terminales o IP´s involucradas en el proceso, etc.)

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Confidencialidad: Proteger la información de su revelación no autorizada. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Cuenta: Mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.

Custodio Técnico: Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: Acceso, Modificaciones, Borrado) que el propietario de la información haya definido, con base en los controles de seguridad disponibles en la organización

Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Disponibilidad: Los recursos de información sean accesibles, cuando estos sean necesitados.

Encriptación Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

Integridad: Proteger la información de alteraciones no autorizadas por la organización. Impacto: consecuencia de la materialización de una amenaza.

ISO: (Organización Internacional de Estándares) Institución mundialmente reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas

Outsourcing: Contrato por servicios a terceros, tipo de servicio prestado por personal ajeno a la institución.

Propietario de la Información: Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida

Responsabilidad: En términos de seguridad, significa determinar que individuo en la institución, es responsable directo de mantener seguros los activos de cómputo e información.

Servicio: Conjunto de aplicativos o programas informáticos que apoyan la administrativa de los puntos de venta, sobre los procesos diarios que demanden información o comunicación de la entidad.

Soporte Técnico: (Personal en Outsourcing) Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la institución.

Riesgo: posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

Terceros: Contratistas, proveedores de software y usuarios de la red, que tengan convenios empresariales o profesionales con la entidad.

Usuario: Cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga una especie de vinculación contractual o laboral con la entidad.

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

ANEXO I

Yo _____, identificado(a) con la Cédula de Ciudadanía No._____ de _____, me comprometo a cumplir con los siguientes consensos que apliquen en mi condición de empleado, contratista o usuario externo de la SCRD.

1. Contraseñas

1.1. Mi usuario y contraseña serán emitidos y comunicados en línea con los procedimientos de la SCRD.
1.2. Cambiaré mi contraseña temporal inicial dentro de las siguientes 8 horas hábiles después de recibida, al primer inicio de sesión.
1.3. Seleccionaré y usaré una contraseña de al menos 8 caracteres alfanuméricos, de acuerdo con los requerimientos definidos por el área de Grupo Interno de Sistemas y en lo posible no haré uso de: nombres, fechas de nacimiento, números de teléfonos, palabras del diccionario, y números o letras repetidas consecutivas.
1.4. Mantendré mi contraseña secreta; bajo ninguna condición la divulgaré, no la compartiré con nadie, ni en forma verbal o escrita, ni la dejaré en un lugar donde pueda ser registrada o grabada.
1.5. Cambiaré mi contraseña por lo menos cada 35 días y no intentaré volver a usar las contraseñas anteriores en secuencia y/o la cambiaré más frecuentemente si tengo evidencia de que ha habido un evento donde quedó comprometida la seguridad de sistema o activo informático.
1.6. No usaré la misma contraseña en la SCRD y en mis actividades personales.

2. Políticas de escritorio, protectores de pantalla y reproducción de la información.

2.1. Tomaré las precauciones necesarias para que nadie acceda a mi sesión de trabajo cuando no me encuentre. Para lo cual en cada oportunidad que deba ausentarme del puesto de trabajo bloquearé la estación, cuando finalice mis labores o por alguna circunstancia deba abandonar las instalaciones de la entidad, apagaré el equipo (CPU y monitor).

2.2. Cumpliré los requisitos legales y reglamentarios relacionados con las políticas de privacidad y protección de datos, por lo tanto, no emitiré copias, ni divulgaré o emplearé indebidamente, ni reproduciré por medio alguno la información contenida en los aplicativos de la SCRD, salvo los casos en que expresamente el personal vinculado sea facultado para ello.

2.3. No divulgaré o emplearé el contenido de un documento que deba permanecer en reserva de acuerdo con el Código Penal Colombiano.

3. Hardware.

3.1. Cuando requiera la asignación, traslado o devolución de un equipo de cómputo, solicitaré al área de Grupo Interno de Sistemas la asignación, autorización o retiro correspondiente.
3.2. En caso de requerir el cambio de un equipo de cómputo o una parte, solicitaré al área de Grupo Interno de Sistemas el cambio respectivo.
3.3. En caso que el equipo de cómputo deba ser retirado de las instalaciones de la SCRD, solicitaré autorización previa respectiva, con el visto bueno de la persona que tenga a cargo el equipo.
3.4. Informaré oportunamente al área de Grupo Interno de Sistemas cualquier falla en los equipos de cómputo a mí asignados.
3.5. Los equipos de cómputo a mí asignados, los destinaré exclusivamente para el cumplimiento de las funciones de la entidad.
3.6. Responderé por el inventario de Hardware y Software asignados.

4. Aplicativos

4.1 Manifiesto que conozco a cabalidad que el acceso y uso de los aplicativos es exclusivamente durante la vigencia de la vinculación con la entidad, acorde con las actividades que así lo ameriten.
4.2. Guardaré y divulgaré los principios de confidencialidad de la información que se proporciona a través del presente acuerdo.
4.3. Mantendré mi contraseña secreta; bajo ninguna condición la divulgaré, no la compartiré con nadie, ni en forma verbal o escrita, ni la dejaré en un lugar donde pueda ser registrada o grabada. Por lo que me haré responsable de todas las actividades realizadas con mi cuenta asignada.
4.4. No ingresaré sin autorización a los Sistemas informáticos de la SCRD que estén protegidos con medidas de seguridad.
4.5. Acepto que la SCRD podrá realizar controles y monitoreo de la actividad computacional para garantizar los niveles adecuados de seguridad informática.
4.6. Aceptaré cualquier cambio del perfil de acceso cuando así lo disponga el supervisor de mi contrato o a mi Jefe Inmediato por cambio de mis actividades.
4.7. Acepto que el Administrador del Aplicativo procederá con el bloqueo de la cuenta cuando éste evidencie el no uso dentro del tiempo definido por el programa.
4.8. Garantizaré que todo ingreso, modificación, novedad o cualquier cambio de información que llegare a realizar sobre los Sistemas de Información lo realizaré exclusivamente basado en el soporte documental que así lo respalde.

4.9. Cuando se presente bloqueo de la cuenta de usuario, informaré al Administrador del aplicativo para que adelante las acciones que estime pertinentes.

5. Software

5.1 No borraré, deshabilitaré o sobrescribiré el Software de la SCRD instalado en el equipo de cómputo a mí asignado, incluyendo: antivirus, cortafuegos servicios de actualización automática; como tampoco descargaré de Internet, ni instalaré ningún software que no tenga licencia legítima y válidamente autorizada en el equipo de cómputo a mí asignado por el Área de Gestión de Sistemas e Informática.
Parágrafo: Esta prohibición incluye "freeware, shareware, screensavers, toolbars" y cualquier programa disponible. Todas las instalaciones de software que requiera, las solicitaré únicamente al área de Grupo Interno de Sistemas. Daré buen uso al correo electrónico y de Internet, de conformidad con las políticas de seguridad establecidas para ello.

6. Control de datos y legislación

6.1 Cumpliré los requisitos legales y reglamentarios relacionados con las políticas de privacidad y protección de datos, en el equipo de cómputo a mí asignado.

7. Backup y clasificación de la información

7.1 Reconozco que soy responsable de realizar backup a la información crítica para la SCRD existente en mi estación de trabajo.
7.2 Tengo conocimiento de la existencia de políticas de almacenamiento en el servidor de archivos o en medios extraíbles, y conozco donde debo guardar información importante para la Entidad.

8. Mantenimiento

8.1 Velaré por la seguridad física del equipo de cómputo a mi asignado y reportaré al Área de Gestión de Sistemas e Informática cualquier falla que afecte esta seguridad.

9. Monitoreo de Auditoria y seguridad

9.1 Estaré expectante de cualquier violación de la seguridad y comunicaré de manera inmediata al supervisor de mi contrato, a la Coordinación del Área de Gestión de Sistemas e Informática o a quien sea una autoridad en ésta.

10. Revocación y cambio de los perfiles de acceso

10.1 En caso de detectar operaciones o uso indebido de la cuenta por parte de algún usuario, procederé a informar la situación por escrito al supervisor de mi contrato o a mi Jefe Inmediato.

10.2 Aceptaré cualquier cambio de perfil de acceso en caso de ser requerido por la SCRD.

El presente acuerdo se firma a los _____ días de mes de _____ de 20___.

Firma Director o Asignado:_____

Firma del Usuario: _____

Fecha de Retiro y/o Terminación de Contrato (día/mes/año): _____

ANEXO II - ATRIBUTOS CLASIFICACION ACTIVOS INFORMACION

Atributos de Clasificación

A cada activo de información se le relaciona uno o más atributos, los cuales permiten identificar su sensibilidad y justificar el valor asignado al activo y adicionalmente permitirán obtener elementos que permitan darle un tratamiento adecuado. Los atributos asociados al activo de información y que se tiene como información de referencia en la matriz de inventario y clasificación de activos de información es la siguiente:

A1: Activo de información de clientes o terceros que debe protegerse, de accesos no autorizados, pérdida de integridad o indisponibilidad.
A2: Activo de información que debe ser restringido a un número limitado de funcionarios.
A3: Activo de información que debe ser restringido a personas externas a la SCRD.
A4: Activo de información que puede ser alterado o comprometido para fraudes ó corrupción.
A5: Activo de información que es muy crítico para las operaciones internas de la SCRD.
A6: Activo de información que es muy crítico para la prestación de servicio a terceros, tales como ciudadanos, organismos de control, u otras organizaciones.
A7: Activo de información que ha sido declarado de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica.