



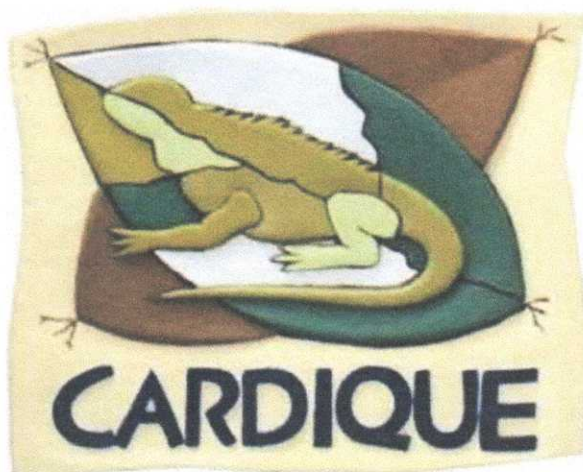
MANUAL DE POLITICAS DE SEGURIDAD DE LA
INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 1 de 41



Manual de Políticas de Seguridad de la Información

NOVIEMBRE DE 2018



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 2 de 41

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	5
2. OBJETIVO.....	5
3. ALCANCE Y APLICABILIDAD DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN.....	5
4. TERMINO Y DEFINICIONES.....	6
5. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.....	12
6. POLITICA DE LA ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN.....	12
6.1 Política de la Estructura Organizacional de seguridad de la información.....	12
6.2 Política de seguridad y clasificación de la información.....	15
6.3 Política de la gestión de activos de la información.....	18
6.4 Política de uso de estaciones cliente.....	18
6.5 Política de seguridad física.....	19
6.6 Política de uso de discos de red o carpetas virtuales.....	21
6.7 Política de seguridad de los centros de datos y centros de cableado.....	21
6.8 Política de uso de los dispositivos móviles.....	22
6.9 Política de seguridad del recurso humano.....	24
6.10 Política de uso del internet.....	25
6.11 Política de establecimiento, uso y protección de claves de acceso.....	26
6.12 Política de seguridad en medios de información y equipos.....	27



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

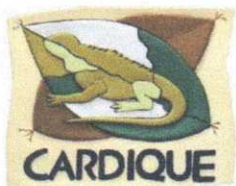
PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 3 de 41

6.13	Política de escritorio y pantalla limpia.....	28
6.14	Política de uso de impresoras y servidores de impresión.....	29
6.15	Política de adquisición, desarrollo y mantenimientos de sistemas de información.....	30
6.16	Política de respaldo y restauración de información.....	31
6.17	Política de uso de correo electrónico.....	32
6.18	Política de las comunicaciones.....	33
6.19	Política de administración y publicación de la página web.....	34
6.20	Política de seguridad y uso de redes sociales.....	35
6.21	Políticas específicas de funcionarios y contratistas del área de tecnologías y sistemas de información.....	35
6.22	Política de tercerización u outsourcing.....	36
6.23	Política de gestión de los incidentes de seguridad de la información.....	37
6.24	Política de control de software.....	37
6.25	Política de vulnerabilidad.....	38
6.26	Política específicas para usuarios.....	38
6.27	Política de retención y archivo de datos.....	39
7.	Procedimientos que apoyan la seguridad de la información.....	40
7.1	control de documentos.....	40
7.2	control de registros.....	40



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 4 de 41

7.3 mejora continua.....	40
7.4 revisión del manual de políticas de seguridad de la información.....	40
8. Marco Legal.....	41
9. Requisitos técnicos.....	41
10. Responsable del documento.....	41



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 5 de 41

1. INTRODUCCIÓN

La Corporación Autónoma Regional del Canal del Dique CARDIQUE elabora este manual con la finalidad de establecer políticas que integren la gestión de la seguridad de la información enfocadas a dar cumplimiento a la normativa legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno en Línea (GEL) del ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, pretendiendo implementar reglas que permitan proteger la confidencialidad, integridad y disponibilidad de la información como un activo de alta importancia para la entidad.

2. OBJETIVO

El presente documento define los lineamientos que debe seguir la Corporación Autónoma Regional del Canal del Dique CARDIQUE, con relación a la Seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

3. ALCANCE Y APLICABILIDAD DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Estas políticas tienen aplicabilidad a todos los procesos establecidos en la Corporación, con la finalidad de garantizar que los riesgos para la Seguridad Informática sean conocidos, asumidos, gestionados y minimizados por la Alta Dirección, Jefes de Oficinas, Jefes de Áreas, funcionarios, contratistas, terceros y partes interesadas que tengan algún tipo de relación con CARDIQUE, de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riegos, el entorno y la tecnología.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha: 15/11/2018

Página 6 de 41

4. TERMINO Y DEFINICIONES

Acción Correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de una no conformidad, de tal forma que no se vuelva a presentar.

Aceptación del Riesgo: Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.

Activo: Según (ISO /IEC 13335-12004): Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y la cual es necesaria para los procesos misionales de la corporación. Los cuales se pueden clasificar en:

-Datos: Son todos los elementos básicos de la información (en cualquier formato) que se crean, almacenan, tramitan, transfieren y eliminan en la corporación. Ejemplo: archivo de Excel "Matriz Control de Registros.exe".

-Aplicaciones: Es el software utilizado para la gestión de la información.

-Personal: Son todas las personas que tiene de una manera u otra a los activos de información. Ejemplo: funcionarios, terceros, partes interesadas, la comunidad, usuarios en general

-Servicios: Internos que son los que se realizan de forma interna en la corporación, es decir que se suministran información de forma interna y Externa son la información que le suministran a personal externo de la corporación, es decir a los usuarios.

-Tecnología: Son todos los equipos utilizados para gestionar la información y la comunicación interna y externa. Ejemplo: Equipos de Cómputos, Teléfonos, Impresora.

-Infraestructura: Son todos los lugares en donde se instalan los sistemas de información. Ejemplo: Oficina de Contabilidad.

-Equipamiento Auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información. Ejemplo: Aire acondicionado, destructora de papel.

Acuerdo de Confidencialidad: Es un documento firmado por los funcionarios, contratistas, Asesores externos, en la cual manifiestan su voluntad de mantener la confidencialidad de la información de la corporación, comprometiéndose a no divulgar, usar o explotar dicha información a la que tengan acceso en virtud de la labor que desarrollan dentro de la corporación.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 7 de 41

Amenaza: Es un evento que puede desencadenar un incidente en el sistema informático, produciendo daño materiales o perdidas inmateriales en sus activos.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

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

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Contraseña o Clave (Password): Es una forma de autenticación o control de acceso que utiliza información secreta para controlar el acceso hacia algún recurso informático. Puede estar conformado por números, letras y/o caracteres especiales.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 8 de 41

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Evaluación de Riesgo: Todo proceso de análisis y valoración del riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Incluye la valoración de riesgos y el tratamiento de riesgos.

Guías de clasificación de la información: Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking ético: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intención maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 9 de 41

Información confidencial (RESERVADA): Información administrada por la Corporación en cumplimiento de sus deberes y funciones y que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida previa autorización del titular de la misma.

Información confidencial (CONFIDENCIAL): Información generada por la Corporación en cumplimiento de sus deberes y funciones y que debe ser conocida exclusivamente por un grupo autorizado de funcionarios por esta. El acceso a este tipo de información debe ser restringido y basado en el principio del menor privilegio. Su divulgación a terceros requiere permiso titular de la misma y de acuerdos de confidencialidad. Así mismo, su divulgación no autorizada puede causar daños importantes a la Entidad. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.

Información privada (USO INTERNO): Información generada por la Corporación en cumplimiento de sus deberes y funciones, que no debe ser conocida por el público en general. Su divulgación no autorizada no causa grandes daños a la Entidad y es accesible por todos los usuarios.

Información Pública: Es la información administrada por la Corporación en cumplimiento de sus deberes y funciones que está a disposición del público en general.

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes al instituto.

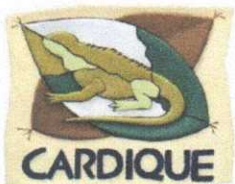
Impacto: medición de los efectos que se generan en el Sistema Informático cuando se materializa una amenaza.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002: 20005 el 1 de julio de 2007.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removable: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **10** de **41**

para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Plan de Contingencia: disponibilidad de recursos para atender oportunamente una eventualidad en el Sistema Informático.

Política de Seguridad Informática: Toda intención y directriz expresada formalmente por la alta dirección, con el fin de asegurar que los recursos y la información soportada en la plataforma informática (programas) de la corporación tenga el acceso y el uso para el que se decidió.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la corporación.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Riesgo: Es la probabilidad de ocurrencia de un hecho favorable o desfavorable que pudiera afectar la Seguridad Informática.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 11 de 41

Seguridad de la información: Según (ISO/IEC 27002:20005): Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Sistema de Información: es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo).

Software: es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un Sistema Informático.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Valoración del riesgo: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Vulnerabilidades: Debilidad en la seguridad de la información de una organización que potencialmente permite una amenaza afecte a un activo. Según (ISO/IEC 13335-1:2004): debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **12** de **41**

5. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CARDIQUE define que la Seguridad de la Información es de gran importancia para el desempeño eficiente de las actividades administrativas, razón por la cual la Alta Dirección demuestra su compromiso a través de los siguientes objetivos de seguridad de la información:

- Controlar las vulnerabilidades y amenazas que enfrentan los activos de información y tecnológicos mediante la elaboración de los mapas de riesgos, para asegurar la confidencialidad, integridad y disponibilidad de la información.
- Gestionar el inventario de los activos informáticos y de información que garantice la identificación, clasificación y el mantenimiento de la información, para lograr su uso apropiado durante todo su ciclo de vida en la Corporación.
- Fortalecer la cultura de seguridad de la información mediante difusión, sensibilización y capacitación de Jefes de Oficinas, Jefes de Áreas, funcionarios, contratistas, terceros y partes interesadas que hagan uso de los activos de la información de la entidad, con el fin de dar tratamiento transparente y correcto de la información
- La revisión y aprobación de las Políticas de Seguridad de la Información incluidas en este manual.

6. POLITICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Política de estructura organizacional de la seguridad de la información

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

6.1.1 Roles y Responsabilidades

Alta Dirección

El Comité de Seguridad Informática (se crea o se modifica); las funciones del comité de Seguridad Informática (o el que haga sus veces), debe ser gestionado, conformado y aprobado por la Alta Dirección



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **13** de **41**

de CARDIQUE, es el responsable de establecer y mantener las Políticas de Seguridad Informática, las normas, directrices y procedimientos de la Corporación.

El Comité de Seguridad Informática (o el que haga sus veces), estará integrado por el Director General, la Secretaria General, el Asesor de Control Interno, los Subdirectores de Áreas, los Jefes de Oficinas y el Profesional del Área de Sistemas, los cuales deberán asegurar el cumplimiento de dichas políticas.

Son responsabilidades del Comité de Seguridad Informática:

- Establecer y aprobar los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo
- Revisión y seguimiento al modelo de gobierno de seguridad de la información a implementar en la Corporación.
- Revisión y valoración de la Política de Seguridad Informática.
- Alineación e integración de la seguridad a los objetivos del negocio.
- Garantizar que la seguridad de la información forme parte integral del proceso de planeación estratégica de CARDIQUE.
- Reportar, a través de reuniones semestrales el estado de la seguridad y protección de la información en la Corporación y la necesidad de nuevos proyectos en temas de seguridad de la información
- Establecer y respaldar los programas de concientización de la Corporación en materia de seguridad y protección de la información
- Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información
- Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.
- Promover explícitamente el apoyo institucional a la seguridad de la información en toda la Corporación.
- Supervisar y controlar los cambios significativos en la exposición de los activos de información a las principales amenazas.
- Revisar y seguir los incidentes de seguridad de la información.

Responsabilidades del Profesional del Área de Sistemas:

- Generar los lineamientos para la gestión de la seguridad de la información y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **14** de **41**

- Presentar ante la Alta Dirección, la actualización de la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- Verificar el cumplimiento de las políticas de seguridad de la información, mediante el monitoreo periódico de los controles de seguridad definidos.

Responsabilidades Oficina de Control Interno:

- Planear y ejecutar las auditorías internas de seguridad de la Información a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos de seguridad de la información y las normativas aplicables.
- Ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte de la seguridad de la Información, con el fin de verificar la eficacia de los planes de acción establecidos a las no conformidades generadas en las auditorías ejecutadas.

Responsabilidades de los Servidores públicos, Proveedores y Partes Interesadas:

- Los funcionarios públicos y personal proveído por terceras partes que tengan relaciones laborales con la Corporación, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares relativos a la seguridad de la información.
- Los servidores públicos, contratistas, terceros y público en general deben garantizar que el acceso a la información y la utilización de la misma sea exclusivamente para actividades relacionadas con funciones propias de la entidad, y que ésta sea utilizada de acuerdo a los criterios de confidencialidad definidos por la Corporación.
- El acceso a los sistemas y recursos de información solamente se debe permitir si existe autorización formal y escrita por parte del jefe inmediato, teniendo en cuenta los siguientes parámetros:
El jefe inmediato solo puede autorizar acceso a información propia del área que coordina y solo podrá asignar privilegios de acceso a los servidores públicos, contratistas y terceros que están bajo su supervisión.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

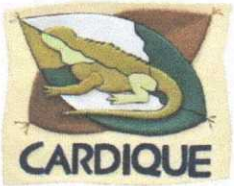
Fecha:15/11/2018

Página 15 de 41

6.2 Política de seguridad y clasificación de la información

CARDIQUE definirá la **Matriz de Información Clasificada y Reservada** con la intención de asegurar que la información reciba el nivel de protección requerido de acuerdo al tipo de clasificación establecido por la Ley 1712 de 2014- Ley de Transparencia y Acceso a la Información y Ley 1581 de 2012 – Protección de datos personales, es por esto que la corporación define los niveles de clasificación de la información, de la siguiente manera:

- 6.2.1 Información Confidencial (RESERVADA): Información que en razón de aspectos legales debe permanecer reservada y puede ser únicamente compartida previa autorización del titular de la misma.
- 6.2.2 Información Confidencial (CONFIDENCIAL): Información que está disponible sólo para un grupo de personas autorizadas en la Corporación (definido por el propietario). El acceso a esta información debe ser estrictamente restringido. Todo material generado durante la creación de copias de este tipo de información (ejemplo, mala calidad de impresión), debe ser destruido.
- 6.2.3 Información privada (USO INTERNO): Información de acceso libre para los empleados de la corporación a través de la intranet. Esta información puede ser revelada a terceros si se ha firmado un acuerdo de confidencialidad.
- 6.2.4 Pública: Información que está disponible para cualquier persona dentro y fuera de la corporación sin ninguna restricción.
 - La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.
 - Si la información no está clasificada como pública, ésta no podrá ser proporcionada a ninguna entidad externa sin un acuerdo de confidencialidad.
 - En ausencia de instrucciones claras o precisas, considerarán la información como de uso interno exclusivamente. Esta política aplica especialmente cuando, por algún motivo, no se ha realizado una clasificación de la información.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **16** de **41**

- No deben enviar información de carácter diferente a Dominio Público por correo electrónico, a menos que se tengan medidas adicionales de protección.
- Toda la información (Dominio Público, Uso Interno y Confidencial) debe estar protegida para evitar que personas no autorizadas la consulten, divulguen o modifiquen sin consentimiento a terceras partes (servidores públicos, prestadores de servicios, entidades externas y personal que realiza alguna actividad dentro de la entidad). Estas entidades tendrán acceso a la información únicamente cuando se demuestre la necesidad de conocer su existencia y cuando se haga a través de una cláusula o contrato de confidencialidad.
- Si se confirma o se sospecha que la información o datos confidenciales o privados, son extraviados o revelados a entidades no autorizadas, el Propietario de la información o quien evidenció el hecho deberá notificar inmediatamente al encargado de la seguridad informática de la entidad, con el objeto de realizar un control efectivo de posibles daños y tomar las acciones necesarias.
- Ningún servidor público, contratista o tercero que tenga alguna relación laboral con la Corporación revelará los controles de seguridad de los sistemas de información y la forma en que están implementados, a menos que se obtenga una autorización previa. Esto incluye: Información que se proporciona en presentaciones, discusiones, o es tratada en diferentes foros que incluya aspectos técnicos de infraestructura.
- La información específica de debilidades en sistemas de Información (como pueden ser la caída de un sistema, falta de un control, etc.), no debe ser distribuida a personas que no demuestren la necesidad de conocer esta información. Es decir, las personas que tengan acceso a este tipo de información, deben saber que es estrictamente controlada, y evitar que sea conocida por entidades que puedan representar un riesgo o comprometer los sistemas de información de la entidad.
- Toda la información clasificada como confidencial y para uso interno, debe ser etiquetada (marcada) con base en estándares definidos. Se buscará que estas etiquetas sean mantenidas en buen estado y visibles de tal forma que se puede identificar la clasificación de la información de la entidad en cualquier momento.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 17 de 41

- Cualquier medio de almacenamiento de cómputo que contenga información confidencial o de uso interno (tales como cintas, discos, y otros), debe ser etiquetado de acuerdo con la clasificación.
- Toda la documentación impresa, escrita a mano o documento legible que contenga información clasificada como confidencial o de uso interno, debe tener una etiqueta que indique el nivel apropiado de sensibilidad con base en la clasificación.

Responsabilidades del Profesional del Área de Sistemas:

- Debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
- Debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son datos de baja o cambian de usuario.

Responsabilidades del Profesional de Archivo

- Debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
- Debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.
- Debe administrar el contrato de almacenamiento y resguardo de las cintas de backup, otros medios de almacenamiento y documentos físicos de la Corporación con el proveedor del servicio.

Responsabilidades de los Servidores públicos, Proveedores y Partes Interesadas:

- La información física y digital de la Corporación debe tener un periodo de almacenamiento de acuerdo con lo establecido en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 18 de 41

- Deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

6.3 Política de la gestión de activos de la información

CARDIQUE como propietario de la información física así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, delegará la responsabilidad a las áreas sobre sus activos de información, afirmando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. puestos de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la Corporación, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los objetivos de la entidad.

Toda la información sensible de la Corporación, así como los activos donde ésta se almacena y se procesa debe ser asignada a un responsable, inventariados y posteriormente clasificados, en la **Matriz Registro de Activos de Información**, es por esto que los propietarios de los activos de información deben llevar a cabo la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

6.4 Política de uso de estaciones cliente

CARDIQUE define lineamientos que orientan que la seguridad es parte integral de los activos de la información, mediante la correcta utilización de estaciones por los usuarios finales.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **19** de **41**

6.5 Política de seguridad física

6.5.1 Política de áreas seguras

CARDIQUE para dar cumplimiento a esta política tiene implementado un sistema de control de acceso, la cual garantiza que todos los servidores públicos, proveedores, partes interesadas, ciudadanos y/o visitantes, que hagan uso de las instalaciones físicas de la Corporación permita su registro de ingreso y salida.

Responsabilidades Alta Dirección:

- Debe controlar el acceso físico, del personal que labora en las áreas, a la Corporación. Dicho control puede ejecutarlo mediante el monitoreo del aplicativo de control de acceso y las cámaras de seguridad.
- Debe velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas, solo sean utilizados por los servidores públicos autorizados y, salvo situaciones de emergencia u otro tipo de eventos, que por su naturaleza lo requieran, estos no sean transferidos a otros servidores públicos de la Corporación.

Responsabilidades del Profesional del Profesional del Proceso de Gestión de Infraestructura:

- Debe proveer los recursos necesarios para proteger, regular y velar por el perfecto estado de los controles de seguridad física, establecidos en la Corporación.
- Debe presentar mejoras a los equipos de seguridad física implantados y, de ser necesario, implementar nuevas estrategias que permitan optimizar, con el fin de perfeccionar la actividad de seguridad física de las instalaciones de la Corporación.
- Debe asegurar mediante revisión aleatoria (Lista de Chequeo-Cronograma de Chequeo) al área en donde se encuentre el Centros de Cableado y/o Cuarto de Servidores, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **20** de **41**

- Debe asegurar mediante revisión aleatoria (Lista de Chequeo- Cronograma de Chequeo) a todo el cableado eléctrico, que está instalado en las áreas físicas de la Corporación, se encuentren en las respectivas canaletas y las mismas, deben estar con sus respectivas tapas de seguridad.

Responsabilidades de los Servidores públicos, Proveedores y Partes Interesadas:

- Todos los servidores públicos, proveedores, ciudadanos y/o visitantes, deben hacer uso del sistema de control de acceso, para ingresar y salir de las instalaciones físicas de la Corporación.
- Todos los servidores públicos, proveedores, ciudadanos y/o visitantes deben portar el carnet, que los identifica como tales. El mismo debe estar en un lugar visible, mientras se encuentren en las instalaciones físicas de la Corporación. En caso de pérdida del carnet de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible **al área de recursos humanos**.
- Todos los servidores públicos, proveedores, ciudadanos y/o visitantes, que ingresen a las instalaciones físicas de la Corporación, no deben intentar ingresar a áreas a las cuales no tengan autorización.
- Los Visitantes, Proveedores y/o Terceros, que ingresen a las instalaciones físicas de la Corporación siempre deberán estar acompañados de un servidor público del área, durante su visita.

Responsabilidades del Profesional del Área de Sistemas

- Debe deshabilitar o modificar de manera inmediata, los privilegios de acceso físico al Centro de Datos, Centros de Cableado, que están bajo su custodia, en los eventos de desvinculación, licencia, vacaciones o cambio en las labores de un servidor público autorizado a ingresar.
- Debe proveer las condiciones físicas y medioambientales necesarias, para asegurar la protección y correcta operación de los recursos de la plataforma tecnológica, ubicados en al Centro de Datos, Centros de Cableado; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **21** de **41**

descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente mediante lista de Chequeo

- Debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente, autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos y correctivos.

6.6 Política para uso de discos de red o carpetas virtuales

CARDIQUE mediante esta política asegura la operación correcta y segura de los discos de red o carpetas virtuales.

6.7 Política de seguridad de los centros de datos y centro de cableado

CARDIQUE para dar cumplimiento a esta política cuenta con área de infraestructura física asignada para la protección la información.

En el área de centro de datos o de los centros de cableados, se presentan las siguientes prohibiciones:

- Fumar dentro del Centro de Datos
- Introducir alimentos o bebidas al Centro de Datos
- El porte de armas de fuego, corto punzantes o similares
- Mover, desconectar y/o conectar equipo de cómputo sin autorización
- Modificar la configuración del equipo o intentarlo sin autorización
- Alterar software instalado en los equipos sin autorización
- Alterar o dañar las etiquetas de la identificación de los sistemas de información o sus conexiones físicas



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **22** de **41**

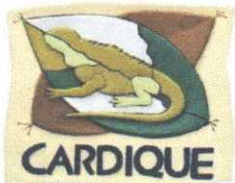
- Extraer información de los equipos en dispositivos externos
- Abuso y/o mal uso de los sistemas de información
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

6.8 Política para uso de dispositivos móviles

La corporación establecerá las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes, "Smart phones", tabletas), entre otros suministrados por CARDIQUE y personales los cuales deben ser exclusivamente utilizados para brindar apoyo a las actividades propias de la entidad, garantizando con esto, que los servidores públicos, proveedores y partes interesadas utilicen responsablemente los servicios y equipos proporcionados por CARDIQUE.

Responsabilidades del Profesional del Área de Sistemas:

- Debe investigar y probar las opciones de protección de los dispositivos móviles corporativos y personales que hagan uso de los servicios proporcionados por la Corporación.
- Debe establecer las configuraciones aceptables para los dispositivos móviles corporativos o personales que hagan uso de los servicios proporcionados por la Corporación.
- Debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles corporativos que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- Debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles corporativos haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **23** de **41**

- Debe configurar la opción de borrado remoto de información en los dispositivos móviles corporativos, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- Debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles corporativos de CARDIQUE; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.
- Debe instalar un software de antivirus tanto en los dispositivos móviles corporativos como en los personales que hagan uso de los servicios proporcionados por la Corporación.
- Debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles corporativos antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Responsabilidades de los Servidores públicos, Proveedores y Partes Interesadas:

- Deben evitar usar los dispositivos móviles corporativos en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- No deben modificar las configuraciones de seguridad de los dispositivos móviles corporativos bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles corporativos.
- Deben cada vez que el sistema de sus dispositivos móviles corporativos notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- Deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles corporativos asignados.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **24** de **41**

- Deben evitar conectar los dispositivos móviles corporativos asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- No deben almacenar videos, fotografías o información personal en los dispositivos móviles corporativos asignados.

6.9 Política de seguridad de los recursos humanos

CARDIQUE tiene como finalidad garantizar la ejecución de las actividades propias de la vinculación laboral, la capacitación, el desarrollo del contrato, el bienestar del personal y en general la gestión del talento humano, acorde con la legislación vigente y orientada a dar cumplimiento a los objetivos misionales de la corporación.

Responsabilidades del Profesional del Área de Talento Humano

- Debe realizar las verificaciones para la veracidad de la información suministrada por el aspirante a ocupar el cargo en la Corporación, antes de su vinculación definitiva.
- Debe certificar que los funcionarios de la Corporación firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a la carpeta de la hoja de vida del contratado.
- Debe convocar a los funcionarios a las charlas y eventos programados como parte del programa de concienciación en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.
- Todos los funcionarios de la Corporación deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 25 de 41

Responsabilidades de los Servidores públicos, Proveedores y Partes Interesadas:

- Deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información

6.10 Política de uso de internet

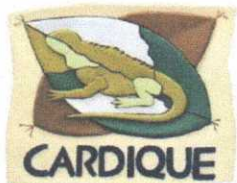
CARDIQUE permite el acceso a servicio de internet a los funcionarios para el desempeño de sus funciones relacionadas con las necesidades del cargo y cumpliendo los lineamientos que garanticen la navegación segura y el uso adecuado de la red.

Los funcionarios con acceso a Internet, al acceder al servicio están aceptando que:

- Serán sujetos de monitoreo de las actividades que realizan en Internet.
- Existe la prohibición de acceso a páginas no autorizadas.
- Se prohíbe la transmisión de archivos reservados o confidenciales no autorizados.
- Se prohíbe la descarga de software sin la autorización correspondiente.
- La utilización de Internet es para el desempeño de su función y no para propósitos personales.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

Responsabilidades del Profesional del Área de Sistemas:

- Debe proveer los recursos para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **26** de **41**

- Debe implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

6.11 Política de establecimiento, uso y protección de claves de acceso

CARDIQUE creará para cada funcionario, usuario y clave de acceso (contraseña) respectiva para poder acceder a la plataforma tecnológica y sistemas de información, garantizando que todos los servidores públicos, proveedores y partes interesadas, que requieran ingresar, se responsabilicen por hacer un uso adecuado y correcto de los usuarios y contraseñas las cuales deben ir acorde con el desarrollo de sus funciones.

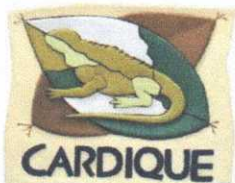
6.11.1 Manejo de Contraseñas para el Administrador de tecnología

El Profesional del Área de Sistemas de la Corporación no debe dar a conocer su clave de usuario a terceros, estas son de uso personal e intransferible. Debe emplearse claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.

El administrador de los sistemas de información de CARDIQUE debe seguir las políticas de cambio de clave y utilizar el procedimiento de salvaguardar o custodiar las claves o contraseñas en un sitio seguro. A este sitio solo debe tener acceso el Profesional del Área de Sistemas.

6.11.2 Usuario y Clave

- Todos los funcionarios que tengan acceso a sus recursos tecnológicos deben disponer de un Usuario y una Clave de carácter privado, personal e intransferible.
- Todo funcionario que acceda a la infraestructura tecnológica de la Corporación debe contar con un Identificador de Usuario (UserID) único y personalizado, por lo cual no está permitido el uso de un mismo UserID por varios empleados.
- Cuando un funcionario olvide, bloquee o extravíe su Clave deberá informarlo al Profesional del Área de Sistemas para que se le proporcione una nueva Clave y una vez que la reciba deberá cambiarla en el momento en que acceda nuevamente a la infraestructura tecnológica.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **27** de **41**

- Está prohibido que las Claves se encuentren de forma legible en cualquier medio impreso y dejarlas en un lugar donde personas no autorizadas puedan descubrirlas.
- Sin importar las circunstancias, las Claves nunca se deben compartir o revelar. Hacer esto responsabiliza al empleado que prestó su Clave de todas las acciones que se realicen con la misma.
- La Clave tendrá una vigencia de 45 días. Finalizando este periodo el empleado recibe una solicitud electrónica de cambio de contraseña. Si el empleado llegara a sospechar que su Clave ha sido descubierta deberá modificarla inmediatamente.
- Los funcionarios no deben guardar almacenar las claves en ningún programa o sistema que proporcione esta la facilidad de ser leídas, computadores sin control de acceso o en lugares donde personal no autorizado tenga acceso.

6.12 Política de seguridad en medios de información y equipos

CARDIQUE para dar cumplimiento a la Política de Seguridad para los Equipos corporativos, implementará la Matriz de Inventario de activos tipo hardware, en la cual debe figurar el propietario de cada activo y su ubicación.

La Corporación pretende garantizar que los recursos tecnológicos reciban una protección óptima, durante las operaciones administrativas que se realicen en la red institucional, permitiendo con esto la preservación de la confidencialidad, integridad y disponibilidad de la información.

- Los medios y los equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.
- El servicio de acceso a internet, intranet, sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la entidad.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **28** de **41**

- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB.
- Se debe implementar el procedimiento para la transferencia de medios físicos.
- La Corporación debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos corporativos, cuenten con la autorización documentada y aprobada previamente por Director General de CARDIQUE.
- La Corporación debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad, posean pólizas de seguro.

6.13 Política de escritorio y pantalla limpia

CARDIQUE establecerá las reglas generales para minimizar el riesgo de acceso no autorizado, pérdida y daño de la información durante la jornada laboral, esta Política será aplicada por los servidores públicos, proveedores y partes interesadas, que tengan acceso a las instalaciones físicas, sistemas de información y equipos de cómputo, la cual deberán conservar el escritorio de los equipos de cómputo libres de documentación sensible y accesos directos, que puedan ser copiada o utilizada por personal que no tenga autorización para su uso o su conocimiento. Además deberán guardar en sitios seguros los dispositivos de almacenamiento que hayan sido suministrados para el desarrollo de sus funciones.

Responsabilidades del Profesional del área de Sistemas

- Mantener actualizado el inventario de activos tipo hardware.
- Verificar que todos los equipos de cómputo se encuentren ingresados al dominio Corporativo.
- Crear, a nivel de controlador de dominio, un bloqueo de sesión de usuario, cuando transcurra cierto y determinado tiempo de inactividad.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **29** de **41**

- Velar que todos los equipos de cómputo sean instalados en el puesto de trabajo, de manera que la pantalla del monitor, no pueda ser visualizada por personal no autorizado.
- Garantizar que la autenticación de usuario sea requerida, cada vez que el equipo de cómputo se encienda, reinicie o bloquee.

Responsabilidades del Profesional del Proceso de Gestión de Infraestructura

- Garantizar que todos los puestos de trabajo y áreas, cuenten con suficientes cajones y/o archivadores, con sus respectivas chapas de seguridad, para almacenar toda la documentación física, que requiera protegerse.

Responsabilidades de los servidores públicos, proveedores y partes interesadas

- No deben ingerir alimentos o bebidas cerca de equipos de cómputo, documentación física y medios magnéticos, así como, evitar manipular líquidos en su cercanía.
- Bloquear la sesión de usuario, cuando se ausente del puesto de trabajo, para proteger el acceso a la documentación digital, aplicaciones y servicios de la Corporación.
- Guardar toda la documentación física y/o medio magnético en cajones, archivadores o sitios seguros, durante su ausencia del puesto de trabajo, manteniendo el mismo, libre de documentación física y medios magnéticos.
- Al imprimir documentos con información sensible de la Corporación, debe ser retirado de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

6.14 Política de uso de impresoras y del servicio de impresión

Asegurar la operación correcta y segura del servicio de impresión.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **30** de **41**

6.15 Política de adquisición, desarrollo y mantenimiento de sistemas de información

CARDIQUE mediante esta política asegura que el desarrollo local o adquisición de software para la corporación deben cumplir con los requisitos de seguridad y calidad, establecidos para tal fin y además deben garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información institucional.

Esta política será aplicada por el área de Informática el cual velará por los Sistemas de Información y los Desarrolladores Internos y/o Externos de la entidad.

Responsabilidades del profesional del área de sistemas

- Debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de acuerdo con las necesidades de la Corporación.
- Debe definir los protocolos para el desarrollo de los sistemas de información de la Corporación.
- Debe velar por el óptimo funcionamiento del software y la información de las aplicaciones implementadas en la corporación contando con el soporte técnico de los desarrolladores internos y/o externos.

Responsabilidades de los Desarrolladores Internos y/o Externos:

- Los Desarrolladores Internos y/o Externos deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles definidos.
- Los Desarrolladores Internos y/o Externos deben garantizar que todo sistema de información adquirido o desarrollado, para la Corporación, utilicen herramientas de desarrollo licenciadas y reconocidas en el mercado.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **31** de **41**

6.16 Política para realizar copia de respaldo y restauración de información

CARDIQUE para dar cumplimiento a esta política provee medios de respaldo necesarios para asegurar que toda la información valiosa y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla, pérdida y/o desastre o catástrofe.

La información de los computadores debe ser periódicamente respaldada en dispositivos destinados para tal fin, para lo cual debe establecerse mediante procedimiento documentado dentro del Sistema de Gestión de la Calidad denominado “procedimientos para copia de respaldo y restauración de información”, el cual establece la prioridad y condiciones bajo las cuales se lleva a cabo el respaldo de la información contenida en los diferentes computadores de la Corporación.

Responsabilidades del profesional del área de sistemas

- Es el responsable de respaldar la información contenida en los Servidores de la Corporación
- Brindará apoyo y asistencia técnica para la instalación de software o hardware de backup
- Debe velar por el óptimo funcionamiento del software y la información de las aplicaciones implementadas en la corporación contando con el soporte técnico de los desarrolladores internos y/o externos.
- Verificará la correcta ejecución de los procesos de backup, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.
- Es el responsable de autorizar una vez haya sido aprobada por la alta dirección la utilización de los dispositivos de almacenamiento externo (Discos Duros Externos, DVD, CD, memorias USB, agendas electrónicas, entre otros), ya que estos pueden ocasionalmente generar riesgos para la corporación al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.
- Debe generar tareas de restauración aleatorias de la información y debe ser documentada mediante la implementación de un formato para guardar evidencias de su realización.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **32** de **41**

- Establecer “Matriz de Riesgos” documentando los diferentes riesgos que pueden ocurrir y las acciones para mitigar o eliminar los riesgos, para el restablecimiento de los sistemas que manejen información crítica, el cual es actualizado frecuentemente para que se ajuste a las condiciones cambiantes de software y hardware.
- Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

6.17 Política de uso de correo electrónico Institucional

CARDIQUE para implementar esta política establece el uso del servicio de correo electrónico institucional, el cual será aplicada por todos los servidores públicos, proveedores, y partes interesadas que tienen alguna relación con la corporación, cumpliendo, con el Procedimiento para la creación de Cuentas de Correo Electrónico Institucional y además, con todos los lineamientos de seguridad que contribuyan a la preservación de la confidencialidad de la información

Responsabilidades del profesional del área de sistemas

- Debe elaborar el Procedimiento para la Creación de Cuentas de Correo Electrónico Institucional y aprobada por la Alta Dirección
- Debe definir los lineamientos para el uso del servicio de correo electrónico institucional
- Debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico institucional.
- Debe garantizar la protección de la plataforma de correo electrónico institucional, contra código malicioso que pudiera ser transmitido a través de los mensajes enviados y recibidos.
- Debe definir y aprobar, el mensaje legal corporativo de confidencialidad para la Corporación, en el correo electrónico institucional



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **33** de **41**

Responsabilidades de los servidores públicos, proveedores, partes interesadas

- La firma electrónica establecida para los emails deberán informar: El nombre de la institución, el cargo del empleado que envía el email, el teléfono y extensión. El tamaño y tipo de fuente utilizada para la misma se deberá ajustar al Manual de Imagen institucional
- Deben ser conscientes que la cuenta de correo electrónico institucional asignada, es de carácter individual; por consiguiente, nadie, bajo ninguna circunstancia, debe utilizar una cuenta de correo diferente a la asignada y aprobada para el desempeño de sus funciones. Como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- No deben enviar cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones, que degraden la condición humana y resulten ofensivas para los servidores públicos, y para la imagen de la Corporación.

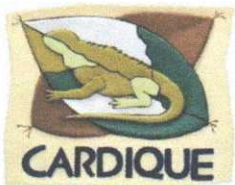
6.18 Política de seguridad en las comunicaciones

CARDIQUE hará cumplimiento de esta política mediante el establecimiento de elementos de controles necesarios que proporcionen la disponibilidad de las redes de datos y de todos los servicios que dependen de ellas; así mismo, vigilará por que se cuente con los dispositivos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Corporación.

Responsabilidades del profesional de Área de Sistemas

- Debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Corporación
- Debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos
- Debe custodiar las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Corporación



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **34** de **41**

- Debe identificar los dispositivos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente
- Debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la Corporación, acogiendo prácticas de configuración segura.
- La Corporación a través de sus funcionarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la misma, en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- Debe instalar protección entre las redes internas de CARDIQUE y cualquier red externa, que este fuera de la capacidad de control y administración de la Corporación
- Debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Corporación.

6.19 Política de administración y publicación de la página web

La Corporación para dar cumplimiento a esta política tiene como objetivo publicar contenidos dirigidos para los funcionarios públicos, proveedores, partes interesadas y Público en general, que apoyen a la misión, visión y políticas corporativas de CARDIQUE, teniendo como resultado, el fortalecimiento de la reputación de la entidad al consolidar la red de sitio web en la fuente de información corporativa oportuna y confiable, dando cumplimiento a la Ley 1712 de 2017 Ley de Transparencia y de Acceso a la Información, mediante la implementación de la **MATRIZ ESQUEMA DE PUBLICACIÓN**.

A fin de asegurar el logro de este objetivo, se han definido los siguientes lineamientos generales para la publicación del sitio web:

- Toda la información será verificada por los editores del sitio para garantizar su veracidad, oportunidad y exactitud antes y durante su publicación.
- La información publicada en el sitio deberá ser de utilidad para los funcionarios públicos, proveedores, partes interesadas y Público en general, siempre buscara destacar los aspectos que favorezcan la buena imagen de la Corporación.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 35 de 41

6.20 Política de seguridad y uso de las redes sociales

CARDIQUE establece las reglas para asegurar una conveniente protección de la información, en el uso del servicio de mensajería instantánea y redes sociales por parte de los funcionarios autorizados por la Alta Dirección.

Para la distribución de la información en las redes sociales que sea generada en el desarrollo de las actividades de la corporación debe ser autorizada por la Alta Dirección.

- La información que se publique por cualquier medio de internet a título personal de un funcionario o contratista de la Corporación, en redes sociales como: twitter, Facebook, YouTube, linkedin, blogs, Instagram, son responsabilidad de la persona que la publique. Por lo tanto la confiabilidad, integridad, disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
- No se debe utilizar el nombre CARDIQUE en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la corporación.

6.21 Políticas específicas para funcionarios y contratistas del área de sistemas

CARDIQUE establece los siguientes lineamientos para funcionarios y contratistas del área de sistemas:

- Los documentos y en general la información de procedimientos, seriales, software, deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad.
- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalaran productos con licencia y software autorizado.
- El profesional del Área de Sistemas se obliga a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **36** de **41**

- El Profesional del Área de Sistemas no utilizará la información para fines comerciales o diferentes al ejercicio de sus funciones.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegurar su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.

6.22 Política de tercerización u outsourcing

CARDIQUE para dar cumplimiento a esta política ha establecido en el Manual de Contratación las directrices legales que blindan ante todo tipo de riesgos y a la vez los criterios de selección para la gestión o ejecución temporal o permanente de una función empresarial por un proveedor externo de servicios. En dicho contrato deberán indicarse, para los casos en que se haga necesario, instrucciones respecto a la protección de datos y normas de privacidad, dado los riesgos potenciales que implica el acceso (Virtual o Físico) de éste a las instalaciones de la Corporación, a la información, a los activos.

Se considera como proveedores de Outsourcing quienes:

- Ofrecen soporte de Hardware y software y al personal de mantenimiento
- Consultores externos y contratistas
- Empresas TI de externalización de procesos empresariales
- Personal temporal
- Si se intercambia información que es confidencial, se deberá generar o exigir un documento/acuerdo de confidencialidad entre CARDIQUE y el Tercero, ya sea como parte del contrato de Outsourcing en sí o un acuerdo de confidencialidad por separado.
- Se deben registrar o documentar los Controles de acceso para restringir la divulgación no autorizada, modificación o destrucción de la información, incluyendo controles de acceso físico y lógico, los procedimientos para conceder, revisar, actualizar y revocar el acceso a los sistemas, datos e instalaciones. Estos controles deben ser definidos entre la Subdirección Administrativa y Financiera y el Área de Sistemas con la aprobación del Director General de la Corporación.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página 37 de 41

6.23 Política de gestión de los incidentes de seguridad de la información

CARDIQUE para garantizar la gestión de incidentes y mejoras en la seguridad de la información, promoverá que los funcionarios públicos, proveedores, y partes interesadas que tiene alguna relación con la corporación reporten al área de sistemas los incidentes referentes con la seguridad de la información, con el fin de tomar oportunamente las acciones correctivas y evitar su recurrencia.

Para el tratamiento de los incidentes de seguridad de la información, el área de sistemas tendrá la responsabilidad de investigar y solucionar los incidentes reportados, y deberá documentarlo e incluirlos en la Matriz de Riesgos con el fin ir escalando los incidentes de acuerdo con su criticidad.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

Responsabilidades del profesional de Área de Sistemas

- Debe garantizar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información identificados y reportados.
- Debe crear la Matriz de Riesgos para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dicha base de conocimiento.

Responsabilidades de Servidores públicos, Partes Interesadas, y Proveedores:

- Deben reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos de la Corporación, con la mayor brevedad posible.
- En caso de identificar la pérdida o divulgación, no autorizada, de la información clasificada con Reservada para la Corporación, deben notificarlo inmediatamente, al Área de Sistemas, para que sea reportado como incidente y se le dé el tratamiento adecuado al caso.

6.24 Política de control de software

CARDIQUE, mediante esta política garantiza que todo el software que están instalados en la plataforma tecnológica de la corporación, se encuentren operando en óptimos niveles de seguridad. Estableciendo procedimiento para controlar la instalación de software operativo, y a la vez asegurar que se cuente con el soporte técnicos de los proveedores de dichos software.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **38** de **41**

La Subdirección de Planeación, en cabeza del área de Sistemas, debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en el Corporación.

Responsabilidades del profesional del Área de Sistemas

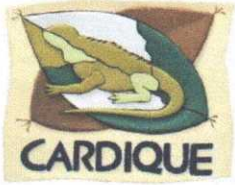
- Debe asegurarse que el software operativo instalado en la plataforma tecnológica de CARDIQUE cuente con el soporte técnico de los proveedores.
- Debe conceder accesos temporales y controlados, a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- Debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado

6.25 Política de vulnerabilidades

La Corporación implementara revisiones periódicas con el fin de revisar, valorar y gestionar las vulnerabilidades identificadas, mediante la aplicación de pruebas de efectividad, con el fin de establecer acciones correctivas para lograr mitigarlo.

Responsabilidades del profesional del Área de Sistemas

- Debe establecer los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.
- Debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- A través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **39** de **41**

6.26 Política específicas para usuarios

CARDIQUE establecerá Procedimiento de Autorización de Acceso a la Red Corporativa realizando la autenticación de usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Corporación. Así mismo, velará porque los funcionarios, proveedores y partes interesadas tengan acceso únicamente a la información necesaria para el desarrollo de sus funciones.

Responsabilidades del profesional de Área de Sistemas

- Debe garantizar la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la Corporación, contemplando la creación, modificación, bloqueo o eliminación de las cuentas de usuarios.
- Debe asegurarse que los usuarios o perfiles de usuario, que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica, sean inhabilitados o eliminados.
- Debe autorizar la creación, modificación o cancelación de las cuentas de acceso de los usuarios, toda vez que Talento Humano notifiquen al área sobre alguna novedad al respecto.

6.27 Política de retención y archivo de datos

CARDIQUE dará cumplimiento a esta política mediante la implementación del programa de gestión documental orientadas en cumplir los lineamientos de las tablas de retención documental exigida por el Archivo General de la Nación, en la cual se establecerá el tiempo que se deberán mantener almacenados los archivos en la Corporación.



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:15/11/2018

Página **40** de **41**

7 Procedimientos que apoyan la seguridad de la información

Los procedimientos describen de forma más detallada las actividades secuenciales que se realizarán, cuales son los recursos utilizados, el método y el objetivo que se quiere lograr, es la base fundamental para dar cumplimiento al Manual de Políticas de Seguridad de la Información.

7.2 Procedimiento de control de documentos y registros

El Objetivo de este procedimiento es el de asegurar el control sobre la creación, aprobación, distribución, utilización y actualización de los documentos y registros utilizados para dar cumplimiento al Manual de Políticas de Seguridad de la Información

7.3 Procedimiento de mejora continua

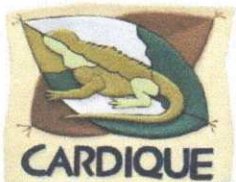
La entidad ha definido el procedimiento de acciones correctivas para reportar las debilidades encontradas para dar cumplimiento a las Políticas establecidas en este Manual. La metodología utilizada son las revisiones aleatorias y auditorías internas programadas, estas debilidades encontradas serán reportadas con la finalidad de evaluar la necesidad de acciones que aseguren la gestión de la seguridad de la información en la Corporación.

7.4 Procedimiento de revisión y aprobación del Manual de Política de Seguridad de la Información

El objetivo fundamental de este procedimiento es realizar revisión y aprobación por parte de la Alta Dirección de la Corporación, a intervalos planificados para verificar su conveniencia, eficiencia y eficacia reflejadas en el cumplimiento de dichas políticas y en los objetivos generales de la Corporación. La gestión del cambio de este Manual se puede presentar por:

- Cambios de normativas aplicables a la seguridad de la información o las aplicables a naturaleza de la Corporación
- Actualización a las políticas contenidas en este manual
- Inclusión de nuevas políticas
- Actualizar lineamientos para dar cumplimiento a las políticas

Se establecerá Acto Administrativo que adopte el Manual de Políticas de Seguridad de la Información y sus procedimientos



MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Versión: 1

Fecha:15/11/2018

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Página **41** de **41**

8 Marco Legal

- Constitución Política de Colombia 1991.
- Ley 594 de 2000 – Ley General de Archivos
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 2000 y ley 1437 de 2011
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”
- CONPES 3854 de 2016 Política Nacional de Seguridad digital

9 Requisitos técnicos

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistema de gestión de la seguridad de la Información

10 Responsable del documento

- Profesional Universitario del Área de Sistemas