POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE

	ELABORADO	REVISADO	APROBADO
NOMBRE	GERARDO CESAR MOSQUERA QUINTERO	JUDITH PARICIA FIGUEROA ALONSO	FERNANDO DE JESÚS JÁCONE GRANADOS
CARGO	ASESOR DE SISTEMAS	SUBGERENTE ADMINISTRATIVA Y FINANCIERA	GERENTE
FECHA	ENERO 2018	ENERO 2018	ENERO 2018
FIRMA			

HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO

MANUAL DE POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FERNANDO DE JESUS JÀCOME GRANADOS
Gerente

GERARDO CESAR MOSQUERA
Asesor De Sistemas

2018

Contenido

Contenido 3
1. OBJETIVO 6
2. ALCANCE 6
3. DEFINICIONES 6
4. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN 7
   a. Política de seguridad de la información 8
   b. Política de privacidad 8
   c. Política de roles y responsabilidades 9
   d. Política de dispositivos móviles 11
5. SEGURIDAD DE LOS RECURSOS HUMANOS 13
   a. Incorporación de la Seguridad en la matriz de Cargos de la entidad 13
   b. Control y Política del Personal 13
   c. De Confidencialidad 13
   d. Selección de personal 14
   e. Términos y condiciones Laborales 14
   f. Entrenamiento, concientización y capacitación 14
   g. Formación y Capacitación en Materia de Seguridad de la Información 15
   h. Procesos disciplinarios 15
6. POLÍTICA DE USO DE CORREO ELECTRÓNICO 16
   a. Usos aceptables del servicio 16
   b. Usos no aceptables del servicio 19
7. POLÍTICA DE USO DE INTERNET 20
   a. Usos aceptables del servicio 21
   b. Usos no aceptables del servicio 22
8. POLÍTICA DE USO DE REDES SOCIALES 23
   a. Usos aceptables del servicio 23
9. POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS 23
   a. Usos aceptables del servicio 24
10. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN 25

a. Esquema de Clasificación de la Información 25
b. Etiquetado y manejo de Información 26
c. Usos no aceptables 27
11. POLÍTICA DE GESTIÓN DE MEDIOS DE ALMACENAMIENTO 27
a. Gestión y Disposición de medios removibles 27
b. Borrado seguro 28
12. POLÍTICA DE CONTROL DE ACCESO 29
a. Control de Acceso a Redes y Servicios en Red 29
b. Gestión de Acceso a Usuarios 30
c. Revisión de los derechos de acceso de los Usuarios 31
d. Retiro de los derechos de acceso 32
13. POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO 32
a. Perímetro de Seguridad Física 32
b. Controles de Acceso Físico 33
c. Ubicación y Protección de los equipos. 34
d. Seguridad de los equipos fuera de las instalaciones 34
e. Seguridad en la reutilización o eliminación de los equipos 35
f. Retiro de Activos 35
14. POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA 35
DESPEJADA 35
15. POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO 36
16. POLÍTICA DE BACKUP 39
a. Registro de Respaldo de Información 41
b. Respaldo de Información para Usuarios Finales 42
17. POLÍTICA DE EVENTOS DE AUDITORIA 42
a. Registro de eventos 43
b. Sincronización de relojes 43
18. POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES 43
19. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES 44

a. Consideraciones de seguridad en los acuerdos con terceras partes 44

20. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN..... 44

a. Reporte sobre los eventos y las debilidades de la seguridad de la información 45

21. POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 46

BIBLIOGRAFIA..... 47

CONTROL DE DOCUMENTOS 48

1. OBJETIVO

Brindar las directrices y lineamientos necesarios que deben seguir los Funcionarios, Colaboradores y Terceros del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE, con el fin de fortalecer la Seguridad de la Información y garantizar la disponibilidad, integridad y confidencialidad de la misma.

2. ALCANCE

Aplica para todos los Funcionarios, Colaboradores y Terceros del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

3. DEFINICIONES

- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

- **La Entidad**: Hace referencia al HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE E.S.E.

4. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Dando cumplimiento a las actividades desarrolladas en la implementación del Modelo de Seguridad y Privacidad de la Información que se encuentra realizando

el HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE, se elaboran una serie de políticas que se describen a continuación:

a. Política de seguridad de la información

El HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la Seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la entidad.

La Gerencia se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de todos los Funcionarios, Colaboradores y Terceros del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

El HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales que haya a lugar, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

Establecer la mejora continua del Sistema de Gestión de Seguridad de la Información, a través de un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE, de una manera contundente, eficiente y efectiva, de la misma forma velar por tomar las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos de acuerdo a la metodología adoptada por la Entidad.

b. Política de privacidad

El HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares

fundamentales de la privacidad de la información como son la finalidad, consentimiento y responsabilidad de información.

La Gerencia se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de privacidad de la información y todas las que se deriven de ella, por parte de todos los Funcionarios, Colaboradores y Terceros del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

El HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE reconoce que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo a la Ley de protección de datos personales 1581 de 2012 decreto 1377 o la que la adicione, modifique o derogue.

c. Política de roles y responsabilidades

Objetivo: Definir los Roles y Responsabilidades en Seguridad de la Información en el HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE

Todos los Funcionarios, Colaboradores y Terceros que ejercen funciones en el HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE y previamente han sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información de la Entidad, son responsables del cumplimiento de las políticas, procedimientos y normatividad vigente definida por el HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

Es responsabilidad de todos los Funcionarios, Colaboradores y Terceros almacenar la información en la carpeta designada para ello (Documentos), los documentos resultado de sus funciones laborales, ya que de esta forma se garantiza las copias de respaldo, lo que no se encuentre allí no queda dentro de la política.

Todos los Funcionarios, Colaboradores y Terceros del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE deben hacer buen uso de la información

que se genera del desempeño de sus funciones laborales y bajo ninguna circunstancia podrán divulgar información con categoría CONFIDENCIAL o RESERVADA en espacios públicos o privados, mediante conversaciones o situaciones que puedan poner en riesgo la seguridad o el buen nombre del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la Entidad.

Todos los activos de información del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE deben tener su custodio, y usuarios que deben estar debidamente identificados, esto de acuerdo a que sólo los Líderes de Proceso definidos en el mapa de procesos de la Entidad, son los que pueden desempeñar las veces de propietarios de activos de información, de acuerdo a esto son los responsables de tomar las medidas necesarias para la protección de la disponibilidad, confidencialidad e integridad de la información de los activos.

La Oficina de Sistemas, Gestión Humana y Jurídica deben definir la Matriz de Roles y Responsabilidades para cada activo de sistemas de información e infraestructura tecnológica, en la cual se deben incluir los roles y sus privilegios, con el fin de crear el procedimiento de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados.

Si después de revisar la solicitud, se identifica que los privilegios solicitados no están definidos en la Matriz de Roles y Responsabilidades de los activos de información, se debe solicitar aprobación por parte del dueño del activo y se ejecutan por la oficina de sistemas.

La oficina de sistemas debe informar a través de los mecanismos de comunicación seleccionados, que el usuario fue creado, modificado o retirado y que fueron asignados los privilegios solicitados.

Se debe capacitar a todos los usuarios solicitantes de accesos a componentes tecnológicos sobre el uso y la responsabilidad que implica contar con esos privilegios.

La Matriz de Roles y Responsabilidades debe ser actualizada periódicamente o cada vez que surja un cambio, de acuerdo a un requerimiento formal por parte del Líder del Proceso o Responsable del Activos de Información.

Todos los requerimientos deben ser solicitados formalmente a través del procedimiento establecido de creación de cuentas de usuarios.

d. Política de dispositivos móviles

Objetivo: Proteger la información almacenada en dispositivos móviles del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE

Se debe llevar un registro y control de todos los dispositivos móviles que posee el HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

Todos los Funcionarios, Colaboradores y Terceros deben hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales.

El uso de dispositivos móviles fuera de las instalaciones sólo es autorizado a través del procedimiento formal de salida de dispositivos.

Todos los dispositivos móviles que almacenen información de HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE deben contar con un sistema de autenticación, como un patrón de movimiento, un código de desbloqueo o una clave.

Todos los equipos de cómputo móviles que almacenen información del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE deben tener instalado un software de antivirus.

Todos los dispositivos móviles que son propiedad del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE pueden estar monitoreados y ser sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

El Funcionario, Colaborador o Tercero responsable del dispositivo móvil debe hacer periódicamente copias de respaldo, en caso de los portátiles deben conectar el quipo mínimo una vez por semana a la red.

Todos los Funcionarios, Colaboradores y Terceros son responsables de garantizar el buen uso de los dispositivos móviles en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

Todos los dispositivos móviles propiedad de los Funcionarios, Colaboradores y Terceros, que requieran tener acceso a los servicios de red, deben solicitar autorización mediante el procedimiento formal de autorización de ingreso a la red y estar debidamente identificados, con el fin de llevar el control y garantizar que se implementen las medidas de aseguramiento necesarias definidas por la Oficina de Sistemas, de esta forma se puede garantizar la preservación de la disponibilidad, confidencialidad e integridad de la información del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

La Oficina de Sistemas puede realizar borrado remoto de los datos en los dispositivos móviles en caso de pérdida o cuando considere necesario de acuerdo a la política de respaldo de información previa autorización del Gerente.

5. SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo: Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja para el HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE., a través de mecanismos de validación y concientización del recurso humano que hará uso de la misma.

a. Incorporación de la Seguridad en la matriz de Cargos de la entidad

Deben ser incorporados los roles y responsabilidades en seguridad de la información, en la matriz de responsabilidades del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

b. Control y Política del Personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación del HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE.

c. De Confidencialidad

Todos los Funcionarios, Colaboradores y Terceros que ingresen a trabajar en LA ENTIDAD, deben firmar como parte de sus términos y condiciones iniciales de trabajo, un Acuerdo de Confidencialidad o no divulgación, en caso de que no estuviere incluido como una cláusula dentro del contrato de prestación de servicios o en el Acta de Posesión del funcionario. Este acuerdo debe incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información, el tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el área de Gestión Humana y Contractual, según sea el caso.

Dentro del mismo acuerdo el Funcionario, Colaborador o Tercero declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del Funcionario, Colaborador o Tercero.

d. Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo a la reglamentación.

Se deben aplicar los controles establecidos por la Entidad para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a la Entidad.

El área de Gestión del Talento humano es la responsable de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación de personal.

e. Términos y condiciones Laborales

Todos los Funcionarios, Colaboradores y Terceros de LA ENTIDAD deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.

Todos los Funcionarios, Colaboradores y Terceros, durante el proceso de vinculación a LA ENTIDAD, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

f. Entrenamiento, concientización y capacitación

Todos los Funcionarios, Colaboradores y Terceros de LA ENTIDAD deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar por el líder del proceso, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Entidad. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

g. Formación y Capacitación en Materia de Seguridad de la Información

Todos los Funcionarios, Colaboradores y Terceros cuando sea el caso, que trabajan para LA ENTIDAD deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información. Dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee la Entidad para el desempeño de sus funciones laborales y contractuales.

h. Procesos disciplinarios

Todos los incidentes de seguridad de la información presentados en LA ENTIDAD deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

En lo pertinente a la violación de las políticas de seguridad de la información de la Entidad, a los Funcionarios, Colaboradores y Terceros, se les aplicará lo

establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

6. POLÍTICA DE USO DE CORREO ELECTRÓNICO

Objetivo: Definir las directrices generales del buen uso del correo electrónico en LA ENTIDAD.

a. Usos aceptables del servicio

Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en LA ENTIDAD y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de LA ENTIDAD.

Todos los Funcionarios, Colaboradores y Terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.

Todos los Funcionarios, Colaboradores y Terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información de LA ENTIDAD.

El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con LA ENTIDAD. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de

seguridad se consideran de propiedad de LA ENTIDAD y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por LA ENTIDAD y deberán conservar en todos los casos el mensaje legal corporativo.

El único servicio de correo electrónico controlado en la entidad es el asignado directamente por la Oficina de sistemas.

Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de los usuarios.

Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo a la Clasificación y Etiquetado de la Información establecida en la entidad.

Todos los Funcionarios, Colaboradores y Terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de LA ENTIDAD, para que de esta forma la Oficina de sistemas realicen el ajuste de permisos requerido.

El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus a la Oficina de Sistemas, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así la Oficina de Sistemas hacen el análisis para evaluar el origen y así tomar las medidas pertinentes.

Cuando un usuario se retire de LA ENTIDAD, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo corporativo, debe abstenerse de continuar empleándolas y debe verificar que su cuenta y acceso a los servicios sean cancelados, de igual forma la oficina de Gestión del Talento Humana deberá reportarla novedad a la oficina de sistemas para realizar el respectivo registro en el sistema y cuenta de correo.

Los mensajes y la información contenida en los buzones de correo son de propiedad de LA ENTIDAD.

Cada usuario se debe asegurar que en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

Cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Las cuentas institucionales (Ejemplo: Autorizaciones, Siau, Cartera, control interno etc.) deben tener una persona responsable que haga depuración del buzón periódicamente.

Todo usuario es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Funcionario, Colaborador o Tercero desconfíe del remitente de un correo electrónico debe remitir la consulta al área de sistemas.

Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la Oficina de Tecnologías de Sistemas actuará según sea el caso.

La Oficina de Sistemas se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos.

Ningún Funcionario, Colaborador o Tercero debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

El Funcionario, Colaborar o Tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario debe notificar a la Oficina de Sistemas, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de LA ENTIDAD.

Toda cuenta de correo es de propiedad de LA ENTIDAD y los buzones que no sean utilizados en un tiempo superior a cuarenta y cinco (45) días se inactivan por el responsable de correo electrónico.

Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.

b. Usos no aceptables del servicio

Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.

Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio de mensajes que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Envió de mensajes que contengan amenazas o mensajes violentos.

Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

Divulgación no autorizada de información propiedad de LA ENTIDAD.

Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico.

Enviar correos masivos, con excepción de funcionarios con nivel de jefes de área o superior, quienes sean previamente autorizados por estos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.

Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

7. POLÍTICA DE USO DE INTERNET

Objetivo: Definir los lineamientos generales para el buen uso del internet y asegurar una adecuada protección de la información de LA ENTIDAD.

a. Usos aceptables del servicio

Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en LA ENTIDAD y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información de la misma.

Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

El navegador autorizado para el uso de Internet en la red de LA ENTIDAD es el instalado por la Oficina de Sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.

No se permite la conexión de módems externos o internos ni ningún otro tipo de dispositivo de redes en la red de LA ENTIDAD, previa solicitud autorizada por la Oficina de Sistemas.

El acceso a internet para cada equipo, depende del rol que desempeñe en LA ENTIDAD y para los cuales este formal y expresamente autorizado.

Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de LA ENTIDAD.

Todos los usuarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet.

LA ENTIDAD se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

Los Funcionarios y Colaboradores y Tercero de LA ENTIDAD no deben asumir en nombre de la entidad, posiciones personales en encuestas de opinión, foros u otros medios similares.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de LA ENTIDAD.

b. Usos no aceptables del servicio

Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

Todos los usuarios invitados que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos de LA ENTIDAD y las emitidas por los entes de control.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

8. POLÍTICA DE USO DE REDES SOCIALES

Objetivo: Definir los lineamientos generales para el uso del servicio de Redes sociales por parte de los usuarios autorizados en LA ENTIDAD.

a. Usos aceptables del servicio

Queda prohibido el uso de las redes sociales dentro de la Institución.

9. POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS

Objetivo: Definir los lineamientos generales para el uso aceptable de los recursos tecnológicos de LA ENTIDAD

a. Usos aceptables del servicio

LA ENTIDAD asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los Funcionarios, Colaboradores y terceros de ser necesario.

El uso adecuado de estos recursos se establece bajo los siguientes criterios:

La instalación de software se encuentra bajo la responsabilidad la Oficina de Sistemas y por tanto son los únicos autorizados para realizar esta actividad.

Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados o autorizados por la Oficina de Sistemas.

La Oficina de Sistemas es la responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en LA ENTIDAD para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Sólo el personal autorizado por la Oficina de Sistemas podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de LA ENTIDAD.

Los Funcionarios, Colaboradores y Terceros de la Entidad son responsables de hacer buen uso de los recursos tecnológicos de LA ENTIDAD y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros Funcionarios, Colaboradores y Terceros, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por LA ENTIDAD.

La información clasificada como personal almacenada en los equipos de cómputo, medios de almacenamiento o cuentas de correo institucionales, debe ser guardada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como “PERSONAL” y no se garantizará el respaldo ni la permanencia de la misma.

Todo activo de propiedad de LA ENTIDAD, asignado a Funcionarios, Colaboradores y Terceros de LA ENTIDAD, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles mediante acta firmada el Funcionario, Colaborador y/o Terceros y el jefe inmediato.

10. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo: Asegurar que la información de LA ENTIDAD es clasificada, con el fin de que sea tratada y protegida adecuadamente.

a. Esquema de Clasificación de la Información

Toda la información de LA ENTIDAD debe ser identificada y clasificada de acuerdo a los niveles de clasificación definidos por la entidad.

La Administración y el Proceso de Gestión Documental son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.

De acuerdo a la clasificación establecida por la entidad y el manejo y almacenamiento de la información, se debe tener en cuenta lo siguiente:

Acceso a la información sólo de personal autorizado.

Llevar un registro formal de acceso a la información.
Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

b. Etiquetado y manejo de Información

Todos los Funcionarios, Colaboradores y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.

Los Directores, Jefes de Oficina, Coordinadores de Procesos deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

Todos los Funcionarios, Colaboradores y Terceros cuando sea el caso de LA ENTIDAD son responsables de la organización, conservación, uso y manejo de los documentos.

Todas las dependencias de LA ENTIDAD deben enviar al Archivo Central la documentación de forma ordenada y organizada, de acuerdo a los tiempos de retención establecidos en la Tabla de Retención Documental y el Manual de Gestión Documental, acompañado del formato único de inventario documental FUID y en medio magnético.

El Archivo Central de LA ENTIDAD recibe las transferencias documentales de acuerdo al cronograma anual de transferencia Documentales.

Los archivos de Gestión de las oficinas de LA ENTIDAD deben custodiar sus documentos de acuerdo a lo especificado en las tablas de Retención Documental.

Se debe definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por LA ENTIDAD.

El etiquetado de información debe incluir la información física y electrónica.

Las etiquetas de la información, se deben identificar y reconocer fácilmente.

Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

c. Usos no aceptables

Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos, solicitudes y denuncias, de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.

Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.

Divulgación no autorizada de los expedientes, documentos, información o archivos.

Realizar actividades tales como borrar, modificar, alterar o eliminar información de LA ENTIDAD de manera malintencionada.

11. POLÍTICA DE GESTIÓN DE MEDIOS DE ALMACENAMIENTO

Objetivo: Proteger la información de LA ENTIDAD velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

a. Gestión y Disposición de medios removibles

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD’s, DVD’s, dispositivos personales “USB”, discos duros externos,

cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de LA ENTIDAD y uso hasta finalización de su contrato o cese de actividades.

Se debe llevar el registro de todos los medios removibles de LA ENTIDAD y mantenerlo actualizado.

Todos los medios removibles deben ser almacenados de manera segura.

Los medios de almacenamiento removibles que se conecten a la red de datos de LA ENTIDAD o que se encuentren bajo su custodia, están sujetos a monitoreo por parte de La Oficina de Sistemas.

Todos los medios de almacenamiento removibles propiedad de LA ENTIDAD, deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc, con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

b. Borrado seguro

Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por LA ENTIDAD para su uso dentro de la red corporativa, deben contar con su respectivo soporte.

Todos los medios de almacenamiento que contengan información de LA ENTIDAD y que salgan de la Entidad y que no se les vaya a dar más uso, deben realizársele el borrado seguro, el cual garantiza que la información no sea recuperable (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores, discos duros externos, etc.).

Los medios de almacenamiento que contengan información de LA ENTIDAD y que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por LA ENTIDAD, el cual garantiza que la información no se es recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).

Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información de LA ENTIDAD.

12. POLÍTICA DE CONTROL DE ACCESO

Objetivo: Definir las directrices generales para un acceso controlado a la información de LA ENTIDAD.

a. Control de Acceso a Redes y Servicios en Red

LA ENTIDAD suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Sólo el personal designado por la Oficina de Sistemas está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de tecnología de LA ENTIDAD.

Todo actividad que requiera acceder a los servidores, equipos o a las redes de LA ENTIDAD, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización la Oficina de Sistemas.

La creación y retiro de usuarios en los sistemas de información en producción debe seguir un procedimiento de Creación, Edición y Eliminación de Usuarios.

Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

b. Gestión de Acceso a Usuarios

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor o igual a 8 caracteres.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la Oficina de Sistemas.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo apliance, impresoras, routers, switch, herramientas de seguridad, etc.).

El acceso a los equipos especializados por medio de la red debe establecerse por medio de métodos de autenticación con protocolos de seguridad.

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.

Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

Reportar a la Oficina de Sistemas sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Reportar a la Oficina de Sistemas sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.

Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada cuatro (4) meses.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por la Oficina de Sistemas.

c. Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a la información y a la Plataforma Tecnológica y de procesamiento de información de LA ENTIDAD, debe ser revisada periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

d. Retiro de los derechos de acceso

Cada uno de los líderes de procesos de la Entidad es responsable de comunicar a la Oficina de Gestión Humana y Oficina Jurídica, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. La Oficina de Gestión Humana es la encargada de comunicar a la Oficina de Sistemas sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

13. POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de LA ENTIDAD.

a. Perímetro de Seguridad Física

Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los Funcionarios, Colaboradores y Terceros autorizados evitar que las puertas se dejen abiertas.

Todos los Funcionarios, Colaboradores y Terceros cuando sea el caso, sin excepción deben portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de LA ENTIDAD.

Los visitantes deben permanecer acompañados de un Funcionario o Colaborador de LA ENTIDAD, cuando se encuentren en las oficinas o áreas donde se maneje información.

Es responsabilidad de todos los Funcionarios, Colaboradores y Terceros de LA ENTIDAD borrar la información escrita en los tableros o pizarras al finalizar las

reuniones de trabajo. Igualmente, no se debe dejar documentos o notas escritas sobre los escritorios al finalizar las reuniones.

Los visitantes que requieran permanecer en las oficinas de LA ENTIDAD por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.

El horario autorizado para recibir visitantes en las áreas administrativas es de 8:00 AM a 12:00 M y 2:00 PM a 5:00 PM. En horarios distintos se requerirá de la autorización de la Gerencia o subgerencia administrativa y financiera.

Los dispositivos removibles, así como toda información CONFIDENCIAL de LA ENTIDAD, independientemente del medio en que se encuentre, deben permanecer guardados bajo seguridad durante horario no hábil o en horarios en los cuales el Funcionario, Colaborador o Tercero responsable no se encuentre en su sitio de trabajo.

Las instalaciones de LA ENTIDAD deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de Funcionarios, Colaboradores y Terceros y visitantes.

b. Controles de Acceso Físico

Las áreas seguras, dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

En las áreas seguras, bajo ninguna circunstancia se puede fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un Funcionarios o Colaboradores del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante

el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

c. Ubicación y Protección de los equipos.

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

d. Seguridad de los equipos fuera de las instalaciones

Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deben ser controlados mediante el cifrado de la información almacenada en sus discos duros, utilizando la herramienta definida por la Oficina de Sistemas.

Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente a la Subgerencia Administrativa y financiera, debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.

Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.

Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de LA ENTIDAD.

e. Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

f. Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado de LA ENTIDAD sin una autorización formal.

Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de LA ENTIDAD.

14. POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA

Objetivo: Definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de LA ENTIDAD.

Todo el personal de LA ENTIDAD debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

Todo el personal de LA ENTIDAD debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.

Todos los usuarios al finalizar sus actividades diarias, deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

15. POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en LA ENTIDAD.

Toda la infraestructura de procesamiento de información de LA ENTIDAD, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de LA ENTIDAD.

Todos los Funcionarios, Colaboradores y Terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de LA ENTIDAD son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

LA ENTIDAD cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por la Oficina de Sistemas.

Los antivirus adquirido por LA ENTIDAD, sólo debe ser instalados por los responsables de la Oficina de Sistemas.

Los equipos de terceros que son autorizados para conectarse a la red de datos de LA ENTIDAD deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados la red de LA ENTIDAD pueden ser monitoreados y supervisados por la Oficina de Sistemas.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores.

La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

Se deben hacer campañas de sensibilización a todos los Funcionarios, Colaboradores y Terceros de ser el caso de LA ENTIDAD, con el fin de generar una cultura de seguridad de la información entre los Funcionarios, Colaboradores y Terceros de LA ENTIDAD.

Los Funcionarios, Colaboradores y Terceros de LA ENTIDAD pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Funcionarios, Colaboradores y Terceros cuando sea necesario siempre podrán consultar a la Oficina de Sistemas sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por LA ENTIDAD, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe informara la oficina de sistemas.

El único servicio de antivirus autorizado en la entidad es el asignado directamente por la Oficina de Sistemas, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por la Oficina de Sistemas, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

La Oficina de Sistemas es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red de LA ENTIDAD.

La Oficina de Sistemas se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

La Oficina de Sistemas se reserva el derecho de filtrar los contenidos que se trasmitan en la red de LA ENTIDAD, con el fin de evitar amenazas de virus.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información deberá ser borrada.

16. POLÍTICA DE BACKUP

Objetivo: Proporcionar medios de respaldo de información adecuados en LA ENTIDAD para asegurar la información crítica y que el software asociado se pueda recuperar después de una falla.

La Oficina de Sistemas, debe realizar periódicamente un análisis de las necesidades del negocio para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.

La Oficina de Sistemas debe disponer y controlar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de LA ENTIDAD.

El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales.

Se debe tener en cuenta los lineamientos de la ley 594 de 2000 o cualquiera que la modifique, adicione o derogue.

Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

Se deben definir procedimientos para el respaldo de la información, que incluyan los siguientes parámetros:

Almacenar en una ubicación remota o externa las copias de respaldo recientes de información.

Se deben asignar los niveles de protección física y ambiental adecuada a la información de respaldo según las normas aplicadas y las especificaciones dadas por el fabricante.

Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.

La Oficina de Sistemas, a través del Administrador de Bases de Datos, de la Red y servidores, debe:

Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.

Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.

Realizar una copia de respaldo diaria de los Servidores de Base de Datos.

Los dispositivos magnéticos que contienen información crítica, deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.

El sitio alterno donde se almacenan las copias de respaldo, debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados. (ARCHIVO)

Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.

La Oficina de Sistemas, debe contar con un juego de Backup necesarios por cada Servidor en el sitio Externo.

a. Registro de Respaldo de Información

Debe existir un procedimiento formal de administración y control de copias de respaldos que permita conocer qué información está respaldado.

La información respaldada debe ser probada como mínimo dos veces al año, asegurando que es confiable, integra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.

Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.

Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.

La Oficina de Sistemas, a través del Administrador de la Base de Datos, de Red y Servidores, debe aplicar los siguientes lineamientos:

Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.

Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.

Validar la integridad y accesibilidad de las backup por lo menos cada cuatro meses.

Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.

b. Respaldo de Información para Usuarios Finales

Todos los usuarios deben almacenar la información resultado de sus actividades laborales en la carpeta “Mis Documentos” a la cual se realiza la copia de seguridad.

Todos los usuarios son responsables de solicitar la realización de los respaldos de información almacenada en los equipos asignados a excepción de las copias ya programadas.

Sera responsabilidad de los usuarios tener disponibles los equipos y en las condiciones requeridas para los días y horas en la que se programó la realización de las copias de seguridad

La Oficina de Sistemas, debe mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad, y otros.

Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado como fuga de información.

Todos los Funcionarios, Colaboradores y Terceros de LA ENTIDAD deben dar estricto cumplimiento a esta política y el que haga caso omiso puede ser sujeto a acciones disciplinarias o civiles.

Es responsabilidad todos los Funcionarios, Colaboradores y Terceros almacenar la información crítica asociada con su labor en la ubicación establecida, para garantizar que la información está siendo respaldada.

17. POLÍTICA DE EVENTOS DE AUDITORIA

Objetivo: Asegurar que los registros de los eventos y las operaciones realizadas sobre los sistemas de información, plataforma tecnológica y gesdion documental

de LA ENTIDAD permitan contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

a. Registro de eventos

Todos los accesos de usuarios a los sistemas, deben ser registrados.

Todos los ingresos de personal realizados a las áreas de archivo deberán ser registradas indicando la persona la fecha, hora y actividad a realizar de acuerdo al formato establecido en el programa de gestión documental.

b. Sincronización de relojes

Todos los relojes de la infraestructura de procesamiento de información de LA ENTIDAD, deben estar sincronizados con la hora legal Colombiana.

18. POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES

Objetivo: Establecer los controles necesarios para proteger la información de LA ENTIDAD transportada desde la red interna.

La Oficina de Sistemas es la responsable de administrar y gestionar la red de LA ENTIDAD.

La Oficina de Sistemas es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

LA ENTIDAD proporciona a los Funcionarios, Colaboradores y Terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos

de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la Oficina de Sistemas.

El trabajo a través de medios remotos a la red de datos de LA ENTIDAD, sólo se permitirá de acuerdo a la Política de Teletrabajo establecida por la Entidad.

19. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES

Objetivos: Establecer los criterios de seguridad la información para la información accedida por los proveedores.

a. Consideraciones de seguridad en los acuerdos con terceras partes

En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar Acuerdos de Confidencialidad sobre el manejo de la información.

Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

20. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Gestionar todos los incidentes de seguridad de la información reportados en LA ENTIDAD, adecuadamente, dando cumplimiento a los procedimientos establecidos.

a. Reporte sobre los eventos y las debilidades de la seguridad de la información

Todos los Funcionarios, Colaboradores y Terceros de la entidad y terceras partes tienen la responsabilidad de reportar a la Subgerencia Administrativa y Financiera de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Escalar los incidentes a niveles superiores en caso de que sea requerido.

Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.

Para el transporte de elementos, se debe llevar la cadena de custodia.

Se deben documentar todos los incidentes de seguridad reportados.

Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

21. POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Objetivo: Garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de LA ENTIDAD.

LA ENTIDAD debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.

Para LA ENTIDAD su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier evento.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deben estar incorporados y definidos en los Planes de contingencias.

BIBLIOGRAFIA

Departamento Administrativo de la Función Pública, Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano.

Modelo de seguridad y privacidad de la información emitido por MINTC

Guías del modelo de seguridad y privacidad

Departamento Administrativo de la Función Pública, Guía para la administración del riesgo.

Departamento Administrativo de la Función Pública, Norma Técnica de Calidad en la Gestión Pública NTCGP 1000:2009.

Departamento Administrativo de la Función Pública, Planeación de los Recursos Humanos-Lineamientos de política, estrategias y orientaciones para la implementación.

Presidencia de la República - Secretaría de Transparencia, Documento “Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano.

Presidencia de la Republica – Alta Consejería Presidencial para el Buen Gobierno y la Eficiencia Administrativa, Modelo Integrado de Planeación y Gestión.

CONTROL DE DOCUMENTOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
01	24/09/2017	GERARDO CESAR MOSQUERA ASESOR DE SISTEMAS	ELABORACION DEL DOCUMENTO INICIAL