ANEXO A

POLITICAS DE SEGURIDAD

Tabla de contenido

1. POLITICAS DE SEGURIDAD 6

1.1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 6

1.2 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN . 8

1.2.1 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS 8

1.2.2 POLÍTICA DE CONTINUIDAD EN LAS OPERACIONES 10

1.2.3 POLÍTICA DE GESTIÓN DE ACTIVOS 12

1.2.4 POLÍTICA DE CONTROL DE ACCESOS 16

1.2.5 POLÍTICA PARA EL USO DE MEDIOS REMOVIBLES 21

1.2.6 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA 23

1.2.7 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO 26

1.2.8 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS 31

1.2.9 POLÍTICAS CONTRA CODIGO MALICIOSO 33

1.2.10 POLÍTICA DE ALMACENAMIENTO Y RESPALDO 37

1.2.11 POLÍTICA DE CONTROL Y GESTIÓN DE LOS SERVICIOS DE RED 42

1.2.12 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN 44

1.2.13 POLÍTICA DE RELACIÓN CON LOS PROVEEDORES 46

1.2.14 POLÍTICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 49

1.2.15 POLÍTICA GENERAL DE PROTECCIÓN DE DATOS HECC COURRIER 50

Lista de Ilustraciones

Ilustración 1. Teclas de Bloqueo 25

Lista de Tablas

Tabla 1. Formato de cabecera Politica General de la Información 6
Tabla 2. Formato de Aprobación Política General de la Información 8
Tabla 3. Formato de Cabecera Política de Seguridad de los Recursos Humanos 8
Tabla 4. Formato de Aprobación Política de Seguridad de los Recursos Humanos 10
Tabla 5. Formato de Cabecera Política de Control de Accesos 16
Tabla 6. Formato de Aprobación Política de Control de Accesos 21
Tabla 7. Formato de Cabecera Política de Seguridad Física y del Entorno 26
Tabla 8. Formato de Aprobación Política de Seguridad Física y del Entorno .. 31
Tabla 9. Formato de Cabecera Política de Gestión de Activos 12
Tabla 10. Clasificación de Información..... 14
Tabla 11. Almacenamiento de Información de acuerdo al tipo. 15
Tabla 12. Formato de Aprobación Política de Gestión de Activos..... 16
Tabla 13. Formato de Cabecera Política de Escritorio y Pantalla Limpia 23
Tabla 14. Formato de Aprobación Política de Escritorio y Pantalla Limpia 25
Tabla 15. Formato de Cabecera Política de Almacenamiento y Respaldo 37
Tabla 16. Tipos de Etiquetado de Medios 40
Tabla 17. Formato de Aprobación Política de Almacenamiento y Respaldo 41
Tabla 18. Formato de Cabecera Política General de Protección de Datos HECC COURRIER 50
Tabla 19. Formato de Aprobación Política General de Protección de Datos HECC COURRIER 54
Tabla 20. Formato de Cabecera Política para el uso de Medios Removibles .. 21
Tabla 21. Formato de Aprobación Política para el Uso de Medios Removibles 23
Tabla 22. Formato de Cabecera Política de Control y Gestión de los Servicios de Red..... 42
Tabla 23. Formato de Aprobación Politica de Control y Gestión de los Servicios de Red..... 44
Tabla 24. Formato de Cabecera Política Contra Código Malicioso 33
Tabla 25. Tipos de Códigos Maliciosos..... 35
Tabla 26. Formato de Aprobación Política contra Código Malicioso 37
Tabla 27. Formato de Cabecera Política de Controles Criptográficos..... 31
Tabla 28. Formato de Aprobación Política de Controles Criptográficos 33
Tabla 29. Formato de Cabecera Política de Transferencia de Información 44
Tabla 30. Formato de Aprobación Política de Transferencia de Información ... 46

Tabla 31. Formato de Cabecera Política para la Gestión de Incidentes de Seguridad de la Información..... 49
Tabla 32. Formato de Aprobación Política para la Gestión de Incidentes de Seguridad de la Información..... 50
Tabla 33. Formato de Cabecera Política de Continuidad en las Operaciones . 10
Tabla 34. Formato de Aprobación Política para la Gestión de Incidentes de Seguridad de la Información..... 12
Tabla 35. Formato de Cabecera Política de relación con los Proveedores..... 46
Tabla 36. Formato de Aprobación Política de relación con los Proveedores ... 48

1. POLITICAS DE SEGURIDAD

La norma ISO/IEC 27001 establece que se deben crear políticas basado en los controles que se deben implementar para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos tecnológicos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

1.1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Políticas de Seguridad de la Información					
Política General de la Información					
Política	IS-00	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 1. Formato de cabecera Politica General de la Información
Fuente: http://www.informationshield.com

PROPÓSITO:

Definir los lineamientos o directrices generales para la protección de los activos de información que orientan los procesos que realiza la organización HECC COURRIER, y de igual manera asignar responsabilidades a los funcionarios, contratistas y terceros los cuales deben cumplir para generar los niveles de seguridad y privacidad de la información determinada por la entidad.

ALCANCE:

Esta política aplica a todos los funcionarios, contratistas o proveedores y terceros de HECC COURRIER.

DETALLE:

La política de seguridad de la organización HECC COURRIER está orientada a gestionar y proteger eficazmente los activos empresariales, especialmente la información durante todo su ciclo (recepción, generación, almacenamiento y eliminación), garantizando la confidencialidad, integridad y disponibilidad de la información para el servicio uso de mensajería por esto se ha decido implementar un sistema de gestión de seguridad de la información y los controles establecidos como respuesta al análisis de gestión de riesgos se establece una metodología de evaluación y tratamiento de los riesgos y en una matriz de evaluación y gestión de riesgos.

Todo sistema se apoya en sus empleados y en una cultura de seguridad a través de la concientización y formación dentro de un contexto estratégico y organizacional como parte del SGSI. HECC COURRIER se compromete a

adoptar dentro de su alcance, cuantas medidas de índole humano, técnico, disciplinario y organizacional, sean requeridas para garantizar que el sistema es congruente con los objetivos estratégicos empresariales y cumple con los requerimientos legales, contractuales, regulatorios, de seguridad, de continuidad de negocio y las expectativas de las partes interesadas.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial al sistema de gestión de la seguridad de la información, o cuando se identifiquen cambios en el negocio, en el sistema de gestión, en sus objetivos, o cuando se detecte alguna condición que afectan la política, para garantizar que es adecuada y mejora continuamente al igual que el sistema.

SANCIONES:

La empresa HECC COURRIER debe implementar sanciones contra empleados y terceros que violen las normas escritas. Como primera medida a faltas suponiendo que la acción es involuntaria o accidental, primeras violaciones de las políticas o procedimientos de seguridad de la información debe tener como resultado una advertencia. Segundas violaciones que implican la misma materia debe resultar en una carta que se colocan en el archivo personal del trabajador involucrado. En tercer lugar, violaciones que implican la misma materia deben resultar en una suspensión de cinco días sin pago. Cuarto violaciones que implican el mismo debe resultar en el despido. Violaciones dolosos o intencionales, sin importar el número de violaciones, pueden dar lugar a medidas disciplinarias hasta e incluyendo el despido inmediato.

EXCEPCIONES:

Todos los empleados de la empresa HECC COURRIER responsables de la seguridad de la información deben presentar una solicitud por escrito de excepciones para justarse a las políticas de seguridad de la información. Estas excepciones deben ser aprobadas por unos miembros de la alta gerencia.

EXÁMENES DE LAS POLÍTICAS:

Los documentos de política de seguridad de información escrita en la empresa HECC COURRIER deben ser revisados anualmente por un equipo integrado (como mínimo) de los miembros del área de sistemas, los gerentes y los directores de recursos humanos.

ASIGNACIÓN DE LOS RESPONSABLES:

Responsabilidades del propietario o dueño

Los propietarios de la información son los jefes de departamento, los miembros del equipo de alta dirección, o sus delegados dentro de la empresa HECC COURRIER que cargan con la responsabilidad de la adquisición, desarrollo y mantenimiento de aplicaciones de producción que procesan la información de la empresa HECC COURRIER. Las aplicaciones de producción son programas

informáticos que proporcionan regularmente informes de apoyo a la toma de decisiones y otras actividades empresariales. Toda la información sistema de aplicación de producción debe tener un propietario designado. Para cada tipo de información, propietarios designan la clasificación de sensibilidad relevante, designar el nivel apropiado de criticidad, definen qué usuarios tendrán acceso, y aprobar las solicitudes de diversas formas en que se utilizó la información.

Responsabilidades del usuario

Los usuarios son responsables de familiarizarse con y cumplir con todas las políticas de la empresa HECC COURRIER, procedimientos y normas que se ocupan de la seguridad de la información. Las preguntas sobre el manejo adecuado de un tipo específico de información deben dirigirse a cualquiera de la entidad depositaria o el propietario de la información involucrada.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política General de Sistemas de información	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política General de Sistemas de información	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER	Política General de Sistemas de información	Mayo de 2018	

Tabla 2. Formato de Aprobación Política General de la Información
Fuente: http://www.informationshield.com

1.2 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas específicas de seguridad de la información se han determinado de acuerdo a los controles previamente analizados y a los riesgos sobre todo que se han identificado durante la gestión de la seguridad. Se detallan tales políticas de la siguiente manera:

1.2.1 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

Políticas de Seguridad de la Información					
Política de Seguridad de los Recursos Humanos					
Política	IS-01	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 3. Formato de Cabecera Política de Seguridad de los Recursos Humanos
Fuente: http://www.informationshield.com

PROPÓSITO:

Reducir los riesgos causados por fallas humanas e incentivar el un correcto uso de los recursos informáticos, así como orientar y concienciar sobre la importancia de la aplicación de las políticas de seguridad e información precisa de incidentes para ser

corregidos en la forma correcta.

ALCANCE:

Esta política se debe aplicar a todo el personal de la organización, interno y externo

DETALLE:

La empresa antes de la vinculación laboral se tiene que documentar los roles y obligaciones que estos van a ejercer. En la selección de los empleados se tiene que revisar antecedentes (hoja de vida, experiencia laboral, se deberán revisar antecedentes con la justicia). Términos y condiciones laborales: Tanto para funcionarios como para contratistas estos deben conocer los términos y las condiciones del contrato laboral elaborando énfasis en los aspectos relativos a la seguridad, la confidencialidad y se debe revisar que los contratos estén diligenciados en su totalidad. (El contrato debe contener, derechos, deberes, responsabilidades, estar de acuerdo a la ley y posibles sanciones por incumplimiento).

La organización deberá capacitar y comunicar sobre las políticas de seguridad establecidas en la organización, así mismo capacitará y comunicará cuando se presenten cambios y modificaciones. Todas estas actividades del programa de toma de conciencia, se deberían programar en un periodo cada 3 meses, de preferencia con regularidad, de manera que las actividades se repitan y abarquen a nuevos empleados y contratistas. Toda esta formación de conciencia también se debería actualizar regularmente, de manera que permanezca en línea con las políticas y procedimientos organizacionales, y se debería construir con base en las lecciones aprendidas de incidentes de seguridad de la información. Las campañas de concientización se deben considerar diferentes formas de educación y formación, por ejemplo, conferencias o estudio por cuenta propia.

HECC COURRIER administra de forma correcta la finalización del contrato o canje de contrato y una vez finalizado el contrato se debe verifica la terminación temporal de los servicios, el reintegro de los activos, reposición de documentos, dispositivos (pc, celulares, usb etc), se debe verificar y gestionar el cambio de contraseñas.

RESPONSABILIDADES

La Gestión de los recursos humanos

El área de gestión humana o recursos humanos es el encargado de seleccionar el personal, informara, capacitara y establecerá acuerdos de confidencialidad y de cumplimiento de todas las políticas de seguridad con el personal que ingrese a la empresa.

Responsable de la Alta Gerencia

La alta gerencia es la encargada de establecer términos y condiciones laborales;

mediante cláusulas en los contratos los acuerdos de confidencialidad y cumplimiento de políticas de seguridad con todo el personal y con terceros o proveedores.

Responsable de la seguridad de la información: Se encargará de capacitar y concienciar al personal con asesoría de profesionales especializados, sobre el uso correcto de los recursos informáticos y el cumplimiento de las políticas de seguridad, así como de los acuerdos de confidencialidad.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de seguridad de los recursos Humanos	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Angel Leguizamón	Política de seguridad de los recursos Humanos	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER	Política de seguridad de los recursos Humanos	Mayo de 2018	

Tabla 4. Formato de Aprobación Política de Seguridad de los Recursos Humanos
Fuente: http://www.informationshield.com

1.2.2 POLÍTICA DE CONTINUIDAD EN LAS OPERACIONES

Políticas de Seguridad de la Información					
Política de Continuidad en las Operaciones					
Política	IS-14	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 5. Formato de Cabecera Política de Continuidad en las Operaciones
Fuente: http://www.informationshield.com

PROPÓSITO

Asegurar el funcionamiento continuo de la organización.

ALCANCE

Esta política se debe aplicar a todos los procesos críticos, prioritarios o del negocio de la organización.

DETALLE

- ✓ El área de Sistemas y el área administrativa y financiera serán los encargados de identificar los procesos críticos, asegurarse de que todos los empleados de la empresa comprendan y conozcan los riesgos, elaborar y documentar una estrategia de continuidad del negocio y proponer la adquisición de pólizas y seguros.

- ✓ Antes de elaborar el plan de contingencia el área de Sistemas y el área administrativa y financiera deberán identificar los eventos o amenazas, evaluar los riesgos e identificar controles preventivos. Todo esto debe estar debidamente documentado**.**
- ✓ El área de Sistemas y el área administrativa y financiera deberá realizar la guía de contingencia que debe especificar los siguientes aspectos: los responsables de los procesos de emergencia, definir acciones y correctivos, implementar procedimientos de emergencia, documentar estos procedimientos e instruir al personal; actualizar constantemente el plan de contingencia.
- ✓ Se debe especificar claramente los requisitos y condiciones para su puesta en marcha, los responsables y los requerimientos. Además, se tiene que prever las condiciones de implementación, establecer los procesos de emergencia, y las acciones a realizarse, describir los procesos de recuperación, definir un cronograma de mantenimiento y documentar las responsabilidades y funciones de las personas. (elaborar un documento muy completo del plan de contingencia.).
- ✓ Es responsabilidad de cada uno de los empleados conocer y entender la documentación de su proceso y en caso de tener dudas o querer una explicación detallada, se deberá solicitar una capacitación al área de Sistemas.
- ✓ Para el área de operaciones se cuenta adicionalmente con un plan de continuidad de negocio.
- ✓ La alta gerencia debe identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad

RESPONSABILIDADES

- ✓ El área de Sistemas se encargará de establecer los procedimientos dirigidos a cumplir con todas las directrices y restricciones legales, así mismo de realizar revisiones periódicas a la empresa para verificar el cumplimiento de las políticas de seguridad, solicitar auditorias periódicas, documentar y dar a conocer los requisitos normativos.
- ✓ Los funcionarios y jefes de cada área están obligados a tener el conocimiento y dar a conocer, cumplir y hacer cumplir la presente política y la normativa vigente.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política para la Gestión de Incidentes de Seguridad de la Información	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política para la Gestión de Incidentes de	Abril de 2018	

	Seguridad de la Información		
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política para la Gestión de Incidentes de Seguridad de la Información	Mayo de 2018	

Tabla 6. Formato de Aprobación Política para la Gestión de Incidentes de Seguridad de la Información
Fuente: http://www.informationshield.com

ACEPTACIÓN DE CUMPLIMIENTO

HECC COURRIER puede realizar inspecciones periódicas, de forma aleatoria y tantas veces como se estime conveniente, con el objeto de verificar el cumplimiento de las políticas establecidas en este documento, el correcto funcionamiento del equipo, las aplicaciones instaladas, la información y archivos contenidos en el disco duro (incluyendo correo electrónico) y el cumplimiento de las demás obligaciones y directrices comunicadas a través de los medios establecidos. Como consecuencia HECC COURRIER eliminará todo contenido no autorizado y podrá imponer las sanciones disciplinarias correspondientes según reglamento interno de trabajo.

1.2.3 POLÍTICA DE GESTIÓN DE ACTIVOS

Políticas de Seguridad de la Información					
Política de Gestión de Activos					
Política	IS-04	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 7. Formato de Cabecera Política de Gestión de Activos
Fuente: http://www.informationshield.com

PROPÓSITO:

Organizar la información de acuerdo a su grado de confidencialidad e integridad, establecer y acondicionar niveles de seguridad y garantizar que los activos de la organización sean protegidos de manera adecuada.

ALCANCE:

La política de gestión de activos está orientada y abarca todos los activos propiedad de HECC COURRIER y de sus clientes.

DETALLE:

Normas generales de uso de los activos

El área de Sistemas es el encargado de la compra, configuración, mantenimiento, puesta en marcha, auditorias, contingencia y monitoreo de los equipos y dispositivos de red y solo los autorizados a esta área podrán modificar

cualquiera de las parametrizaciones de los equipos y dispositivos.

A cada empleado se le asignan los activos requeridos para desarrollar las actividades de su cargo y es su responsabilidad y deber:

- Usar los activos asignados solo para fines laborales
- No modificar o vulnerar los permisos de configuración de los equipos.
- No instalar software sin la debida autorización del área de Sistemas y la Dirección del área.
- No retirar los sellos de seguridad que protegen las partes internas de los activos de HECC COURRIER, este sello solo debe ser retirado por un empleado del área de Sistemas.
- No manipular, intercambiar o destruir las etiquetas de identificación de activos.
- No intercambiar activos como teclado, monitor y demás, sin la debida autorización del área de Sistemas.
- No intentar vulnerar, omitir o alterar las directrices y políticas vigentes de seguridad de la información.
- Proteger los equipos y dispositivos de red contra pérdida, daño, robo o acceso no autorizado a alguno de ellos, manteniendo la seguridad y confidencialidad de la información contenida en el equipo, especialmente cuando se encuentre fuera de las oficinas.
- Respetar las restricciones sobre el consumo de alimentos, fumar o beber cerca de los equipos de suministros y equipamiento como electricidad, aire acondicionado, planta eléctrica y un sistema de alimentación no interrumpida (UPS) o demás relacionadas con la continuidad del servicio.
- En caso de retiro de la organización, regresar al área de Sistemas la totalidad de activos asignados y cumplir con lo establecido en el Paz y Salvo de retiro.

Propiedad de los Activos

En cuanto un empleado de HECC COURRIER recibe un activo para el desarrollo de sus actividades, se convierte en propietario de estos activos y debe evitar su pérdida y protegerlos contra acceso, divulgación, modificación, destrucción o interferencia no autorizada. Asimismo, cuando un empleado inicia sus procesos de inducción y el trabajo productivo, recibe acceso a activos asignados a nivel de área y deberá mantener los mismos cuidados que tiene con los activos directamente asignados.

Todo empleado tiene límites de uso sobre los activos asignados y es prohibido modificar o extralimitar sus permisos o perfiles de acceso, cualquier uso indebido se considera como una falta al reglamento interno de trabajo, asimismo el hecho de no notificar fallas en la asignación de permisos, partiendo de la premisa que en general cada proceso puede acceder a información propia del proceso y no de otros departamentos, inclusive dentro del mismo proceso la autorización de acceso puede ser por cargo, por proyecto o por cliente (lo que no requiera para su trabajo no debería accederlo).

Manejo y Clasificación de la Información

Los empleados de HECC COURRIER conocen y manipulan información durante el desempeño de su cargo; esta información incluye los datos conocidos por ocasión de la prestación de los servicios de mensajería y la documentación generada para soportar, mejorar y controlar los servicios; de igual manera incluye información de las personas naturales vinculadas a HECC COURRIER laboralmente, amparadas por las leyes.

La clasificación que indica los métodos de uso, manejo, almacenamiento y transferencia, entre otros; se rige por la confidencialidad de los datos allí consignados; las categorías son:

CLASIFICACIÓN DE INFORMACIÓN	DEFINICIÓN / ALCANCE
INFORMACIÓN CONFIDENCIAL O PRIVADA	Este tipo de Información involucra al cliente o titular de la cuenta, ya que la información que se maneja puede afectar la intimidad o recursos que tiene. La información manejada de correspondencia será confidencial o privada. Esto mismo afecta a los administradores de las plataformas quienes en su acceso deben tener una seguridad para el ingreso. En algunos casos esto se presenta para darle seguridad a áreas que no tienen permisos para ingresar a otras o el uso de sus sistemas, de allí que también se integren en este tipo, aunque estén laborando dentro de la misma entidad.
INFORMACIÓN ESTRATÉGICA O DE USO INTERNO	La información de los trabajadores quienes deben suministrar esta para efectuar sus labores de manipulación y configuración de sistemas y aplicaciones dentro de la entidad. Todo queda constatado en la documentación realizada para el manejo de información en los diferentes casos y procesos, así como también los estándares a trabajar y las políticas, procedimientos que se usan de manera interna.
INFORMACIÓN PUBLICA	Es aquella información que HECC COURRIER tiene a su cargo y que puede publicar sin afectar a los miembros de la empresa ni a los clientes. También la información que se muestre en las plataformas sin necesidad de un login o acceso está dentro de este tipo de información ya que solo se presenta de manera informativa.

Tabla 8. Clasificación de Información
Fuente: Los Autores

Una vez se tiene establecido que tipo de información es conforme a la clasificación, se debe establecer el mecanismo de almacenamiento que dependerá de tres factores fundamentales:

1. El tipo de recursos disponibles
2. La clasificación de la información que se guardará
3. El nivel de disponibilidad y respaldo requerido

Almacenamiento de información correspondiente al tipo de información:

TIPO DE INFORMACION	ALMACENAMIENTO LOCAL	ALMACENAMIENTO EN SERVIDORES DE RED	DISPOSITIVOS EXTERNOS	INFORMACION FISICA
Información Confidencial o privada	X	X		
Información Estratégica o de uso interno	X	X		X
Información Publica	X	X	X	X

Tabla 9. Almacenamiento de Información de acuerdo al tipo.
Fuente: Los Autores

Todos los empleados de HECC COURRIER deben cumplir las disposiciones de seguridad de la información, velando por el cumplimiento de los requisitos de disponibilidad, integridad y confidencialidad. Las políticas, contratos, reglamentos y normas establecen la obligatoriedad que tiene cada empleado de proteger, respetar y cuidar la información de la empresa y de los clientes. Para esto se debe acatar las siguientes obligaciones:

- Realizar las actividades de respaldo (backups) en los periodos estipulados por el área de Sistemas.
- Leer y cumplir los acuerdos de confidencialidad y contratos laborales.
- Cumplir las reglas de procesamiento de la información.
- Cumplir las reglas de manejo de la información en relación con su valor, requisitos legales, sensibilidad y criticidad para HECC COURRIER.
- Cumplir la política de seguridad de la información y las políticas paralelas creadas para garantizar el cumplimiento de los controles
- Cumplir las políticas de manejo de los medios removibles (como son las USBS, teléfonos y discos portátiles…).
- Cumplir las medidas de almacenamiento de la información, para proteger los registros contra pérdida, destrucción o falsificación.
- Cumplir las políticas de uso del correo, portátiles, canal de comunicación e internet.
- No intercambiar información con personas no autorizadas ni por medios no autorizados
- Mantener la política de escritorios limpios, información impresa, papel, dispositivos de almacenamiento removibles, y elementos innecesarios
- Asegurar que el equipo quede BLOQUEADO cada vez que se retire del puesto de trabajo.
- Ser responsable de la confidencialidad y uso exclusivo de las claves a cargo (cumplir las directrices de uso de claves).

RESPONSABILIDADES

Los responsables de la Información: Son los encargados de organizar la información de acuerdo a su nivel de confidencialidad, retener actualizada y documentada la separación y de establecer la concesión de acceso a los

usuarios. Cada área debe vigilar que la clasificación y etiquetar de la información sea correcto.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de Gestión de Activos	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Angel Leguizamón	Política de Gestión de Activos	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Gestión de Activos	Mayo de 2018	

Tabla 10. Formato de Aprobación Política de Gestión de Activos
Fuente: http://www.informationshield.com

1.2.4 POLÍTICA DE CONTROL DE ACCESOS

Políticas de Seguridad de la Información					
Política de Control de Accesos					
Política	IS-02	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 11. Formato de Cabecera Política de Control de Accesos
Fuente: http://www.informationshield.com

PROPÓSITO:

Esta política define los requisitos de control en torno a la gestión del acceso a la información en los sistemas informáticos y de comunicaciones de la empresa HECC COURRIER. También se definen los controles del área de Sistemas frente a la asignación, restricción, bloqueo o eliminación de usuarios, equipos, dispositivos y accesos del personal que ingresa o se retira de HECC COURRIER.

ALCANCE:

Esta política se aplica a todos los sistemas y servicios informáticos de la empresa HECC COURRIER, con un objetivo de tecnología de la información de los empleados y socios de la empresa HECC COURRIER. Aplica para el área de sistemas, Gestión Humana y quienes hagan sus veces en las regionales desde la planeación de contratación hasta el retiro de personal de HECC COURRIER

DETALLE:

Todos los empleados de HECC COURRIER reciben los accesos a los aplicativos y sistemas necesarios para el desarrollo de sus funciones, estos accesos siempre tendrán un mecanismo de identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus

acciones. El área de sistemas es el responsable de controlar los accesos.

Autenticación mediante contraseñas

Las contraseñas son un medio de verificación de la identidad de un usuario antes de darle acceso a un sistema o servicio de información, además funciona como barrera contra accesos no autorizados. Todos los empleados y personal con acceso a los sistemas de la organización son responsables de adherir y cumplir las directrices para manejo de contraseñas y la política de contraseñas vigente para usuarios de: dominio, aplicaciones corporativas, herramientas de trasferencia de información y demás herramientas por las que se maneje información de HECC COURRIER o información de los clientes custodiada por la organización.

Las contraseñas utilizadas por los empleados de HECC COURRIER para habilitar su acceso a sistemas donde se maneje información de la organización o sus clientes debe ser una contraseña de calidad, es decir debe cumplir con los siguientes requisitos:

- El número mínimo de caracteres que compone la contraseña es ocho (8), los cuales deben estar compuestos por al menos 3 de los siguientes 4 grupos de caracteres:
    - Letras mayúsculas, de la A a la Z.
    - Letras minúsculas, de la a a la z.
    - Dígitos en base 10, de 0 a 9
    - Caracteres no alfabéticos (por ejemplo, ¡,#,$,%,&)
- Las contraseñas de los usuarios deben ser cambiadas a intervalos máximos de 30 días, pero los usuarios podrán cambiar las contraseñas en intervalos menores si evidencian una puesta en peligro del sistema o de la contraseña.
- La contraseña no debe:
    - Contener su nombre de usuario.
    - Ser vulnerable al ataque de diccionarios (es decir, que no consistan en palabras idénticas a las incluidas en diccionarios).
    - Contener caracteres idénticos consecutivos, es decir, todos numéricos ni todos alfabéticos, Ej: 12345, AAA, ABC, etc.
    - Basarse en información fácilmente deducible, por ejemplo, información relacionada al nombre, número telefónico, fechas de cumpleaños, etc.
    - Haberse usado con anterioridad en al menos 3 ocasiones.
- La cuenta permanecerá bloqueada por 3 minutos antes de desbloquearse automáticamente cuando el usuario realice más de 3 intentos de inicio de sesión fallidos.

Una contraseña segura debe ser fácil de recordar para evitar que deba escribirla, a manera de ejemplo, usted puede elegir una frase que signifique algo importante, en este caso utilizaremos un refrán comúnmente utilizado “más vale pájaro en mano que cien volando”, es válido que usted incorpore errores ortográficos, o sustituya letras por números en la frase.

Directrices Para Protección de Contraseñas

- Contraseñas temporales: Las contraseñas temporales son aquellas que traen por defecto los dispositivos, los servicios en línea, o las que se asignan por parte del administrador de la herramienta por primera vez, cuando se reasigna un usuario o cuando la contraseña se olvida. Para herramientas administradas por el área de sistemas, la asignación de estas contraseñas temporales debe cumplir con la política de contraseñas vigente y es responsabilidad del usuario cambiar la contraseña temporal o por defecto generada, en el primer registro de inicio.
- Buenas prácticas para el almacenamiento y manejo de contraseñas laborales:
    - Las contraseñas no deben ser almacenadas, es decir ni escritas en papel ni en archivos de software, dispositivos manuales, celulares…, a menos que se puedan almacenar de forma segura o con un formato protegido; métodos adicionales deberán ser aprobados por el área de sistemas y será responsabilidad del director del área.
    - No debe incluir sus contraseñas en ningún proceso de registro automatizado (formularios, esquemas, creación de cuentas, accesos, macros) para acceder automáticamente sin necesidad de digitar la contraseña
    - Si usted necesita acceder a múltiples servicios, sistemas o plataformas, puede utilizar una sola contraseña de calidad que cumpla con las directrices generales, siempre y cuando pueda garantizar que existe un nivel razonable de protección para almacenar la contraseña.
    - Recuerde que debe utilizar varias contraseñas para diferentes entornos, es decir no emplee la misma contraseña para fines laborales y para los que no lo son como personal, familiar, educativo etc.
    - El propietario de las contraseñas es el responsable de mantener su confidencialidad, en caso de incapacidad, vacaciones o cualquier ausentismo que se presente, por ninguna razón se debe proporcionar la contraseña a ninguna persona incluyendo al jefe inmediato y/o compañeros de trabajo. Lo recomendado es que existan otros usuarios que desempeñen la función.
    - En caso de olvidar su contraseña el área de sistemas puede formatearla sin ningún inconveniente; este servicio aplica para correo, equipos, aplicativos y herramientas administradas por HECC COURRIER.

Uso de Dispositivos de Red

HECC COURRIER genera la disponibilidad de los equipos de red necesarios para el funcionamiento y el desarrollo de las actividades de negocio de HECC COURRIER. Cualquier cambio se debe solicitar al área de sistemas con la aprobación de la dirección del área.

Ningún empleado debe traer dispositivos personales que se conecten a las redes de HECC COURRIER. El área de sistemas genera actividades de monitoreo para verificar este cumplimiento y en caso de detectar el uso de un dispositivo

sin autorización se considera como una falta y se gestiona la sanción disciplinaria correspondientes con el jefe del implicado y Gestión Humana.

Controles Técnicos Para El Ingreso Y Retiro de Personal

Actividades Para El Registro de Personal Contratado

1) **Actividades para el registro de Personal Contratado**

- Recibir de gestión humana la planificación para contratación o cambio de cargo con los nombres del o los usuarios seleccionados.
- Crear el o los usuarios de dominio, el cual se realiza a través del Directorio Activo ubicado en el servidor, teniendo en cuenta al momento de la creación lo siguiente:
  a) El estándar de la cuenta para usuario de dominio es la primera letra del nombre de preferencia y el primer apellido.
  b) Si no se puede aplicar la creación al anterior paso se realizará de la siguiente manera:
     i) Primera letra de primer nombre y segundo apellido.
     ii) Primera letra de segundo nombre y primer apellido.
     iii) Primera letra del segundo nombre y segundo apellido.
     iv) Combinar primera letra del primer nombre con primera letra del segundo nombre y primer apellido.
     v) Combinar primera letra del primer nombre con primera letra del segundo nombre y segundo apellido.
- Incluir al o a los nuevos usuarios en los grupos de Directorio Activo ubicado en el servidor que corresponda según el departamento al que ingresa el usuario.
- Crear el nombre del equipo, teniendo en cuenta:
  a) El estándar del nombre del equipo es la primera letra del nombre de preferencia y el primer apellido.
  b) Si no se puede aplicar la creación al anterior paso se realizará de la siguiente manera:
     i) Primera letra de primer nombre y segundo apellido.
     ii) Primera letra de segundo nombre y primer apellido.
     iii) Primera letra del segundo nombre y segundo apellido.
     iv) Combinar primera letra del primer nombre con primera letra del segundo nombre y primer apellido.
     v) Combinar primera letra del primer nombre con primera letra del segundo nombre y segundo apellido.
- Incluir al o los nuevos equipos en la unidad organizacional del Directorio Activo ubicado en el servidor que corresponda según el departamento al que ingresa el usuario.
- Crear la cuenta de correo electrónico, la cual se hace a través de la consola de correo de OFFICE 365, en el cual se le debe aplicar una licencia “Exchange Online plan 1”, para la creación se debe tener en cuenta lo siguiente: El estándar para la creación de cuentas de correo es el siguiente nombre de preferencia.apellido@HeccCourrier.com. Los siguientes campos son de diligenciamiento obligatorio:
  a) Indicar en el campo “Nombre” el nombre de preferencia.

b) Indicar en el campo “Apellidos” los dos apellidos del usuario.
c) Indicar en el campo "Cargo" el cargo que desempeñará el usuario, este lo puede encontrar en el correo que será enviado por Gestión Humana.
d) Indicar en el campo “Área”, el área en el cual se va a desempeñar el usuario.

- Incluir al o los nuevos usuarios en los grupos de Correo que corresponda según el departamento al que ingresa el usuario.
- Asignar el equipo.
- Configurar el software de acuerdo al área.
- Enviar la Hoja de vida equipos HECC COURRIER al usuario responsable de cada equipo para que acepte la asignación. Esta aceptación se guarda de forma digital.
- Realizar el ingreso del equipo del o los usuarios al grupo del antivirus para que apliquen las políticas establecidas.

Actividades para el Retiro de Personal

- Recibir por parte de gestión humana, el paz y salvo de retiro para proceder con la desactivación y eliminación del directorio activo, correo electrónico y grupo de antivirus del o los usuarios correspondientes.
- Verificar que el usuario realice la entrega del equipo según la aceptación realizada en la Hoja de vida equipos HECC COURRIER.
- Realizar la desactivación y cambio de la contraseña del usuario de dominio a través del Directorio Activo ubicado en el servidor.
- Eliminar el usuario de dominio del Directorio Activo ubicado en el servidor e igualmente se elimina de todos los grupos a los que pertenece; después de 5 días.
- Eliminar la cuenta de correo electrónico, la cual se realiza a través de la consola de correo de OFFICE 365 si el usuario posee cuenta allí, teniendo en cuenta los siguientes parámetros:
  a) Para efectos de seguimiento, las cuentas de correo se mantienen durante un mes a partir del retiro del usuario y se le informa al jefe inmediato.
  b) El correo del usuario retirado se redirecciona a la cuenta de correo del usuario que indique Gestión Humana mediante el correo: “Comunicado empleados retirados de HECC COURRIER”.
  c) Cambiar la contraseña para evitar acceso no deseado la cual queda en custodia del área de sistemas
- Actualizar la bitácora de control de cuentas corporativas en donde se evidencia la eliminación de los usuarios de correo, Dominio y cambio de clave de los usuarios SFTP cuando corresponda.
- Guardar el equipo del usuario que se va a retirar, registrando estos activos en el Inventario Software para dejarlos.
- Responder el trámite de Paz y salvo de retiro, indicando claramente las cuentas eliminadas y si se realizó algún tipo re direccionamiento de la cuenta de correo.
- Realizar el backup del equipo el cual solo tendrá alcance para la carpeta HECC y el correo electrónico, esta información se guardará en el tarro ubicado en la caja fuerte. Este proceso tendrá un máximo de 5 días.

RESPONSABILIDADES

Responsable de la seguridad de la información:

Es la persona encargada de establecer directrices, pautas y procesos para los accesos a los sistemas, bases de datos y servicios de información (acceso a los pc, acceso a la red corporativa, acceso a los servidores, acceso a internet, acceso a claves de seguridad, acceso a transacciones etc.). También debe realizar un control de los privilegios de los usuarios y concientizar a los usuarios de la importancia de la no divulgación de las contraseñas. También se encarga de orientar las directrices y procesos para tener sistemas operativos, gateway, firewall, servicios de red etc., debe verificar que todos estos dispositivos y servicios queden debidamente configurados, debe realizar pruebas de escaneo, monitoreo para evitar intromisión. Adicional, debe incentivar y gestionar las contraseñas y privilegios, capacitar y motivar a los usuarios de emplear las medidas de control de acceso (Área de Sistemas).

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de Control de Accesos	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Angel Leguizamón	Política de Control de Accesos	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Control de Accesos	Mayo de 2018	

Tabla 12. Formato de Aprobación Política de Control de Accesos
Fuente: http://www.informationshield.com

1.2.5 POLÍTICA PARA EL USO DE MEDIOS REMOVIBLES

Políticas de Seguridad de la Información					
Política para el Uso de Medios Removibles					
Política	IS-08	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 13. Formato de Cabecera Política para el uso de Medios Removibles
Fuente: http://www.informationshield.com

PROPÓSITO:

HECC COURRIER tiene que crear condiciones que aseguren la confidencialidad, integridad y disponibilidad de la información que se manipula.

ALCANCE:

Establecer las medidas de seguridad orientadas a proteger la multiplicación y expansión de software con código malicioso que son catalogadas como amenazas en poder, certificar el adecuado funcionamiento de los sistemas de información y destinar encargados de adoptar todas las medidas de seguridad necesarias para proteger posibles ataques.

DETALLE:

Buscando evitar la divulgación, modificación, retiro o destrucción no autorizada de información, el departamento de infraestructura controla los permisos de acceso de medios removibles conforme al tipo de información que se manipula en las áreas.

1. **Bloqueo De Puertos Usb Y Unidades Externas**

   HECC COURRIER tiene bloqueados los puertos USB de los equipos que no tienen razones de negocio para mantenerlos habilitados. Cuando un empleado requiera extraer información y tenga razones de negocio para hacerlo tendrá las siguientes opciones**:**

   - ✓ La principal herramienta de transferencia de información segura es el FTPS, todos los empleados pueden disponer de un usuario para transferencia, en caso de no contar con él, solo se debe enviar una solicitud de cambios y o servicios con aprobación del jefe del solicitante.
   - ✓ HECC COURRIER cuenta con unas carpetas compartidas área donde la persona que desee podrá solicitar al área de Sistemas que ubique el archivo en la ruta correspondiente; es preciso mencionar que en las noches se borrará la información almacenada en estas rutas, son lugares de transferencia de información y no de almacenamiento.
   - ✓ Se podrá habilitar los puertos para almacenamiento de información, siempre y cuando se tengan los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información en el medio donde se almacenará, para ello se debe enviar solicitud de cambios y o servicios, con aprobación del jefe
   - ✓ Si la solicitud es para quemado de información, se debe enviar solicitud de cambios y o servicios, con aprobación del jefe que se encarga de garantizar la necesidad de quemado de esta información.
   - ✓ Esta política aplica para los equipos que sean propiedad de HECC COURRIER

RESPONSABILIDADES

El responsable será el encargado de definir los procesos para el control actualización y modificación de los SO (sistemas operativos) tanto de servidores como, ordenadores.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política para el Uso de Medios Removibles	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política para el Uso de Medios Removibles	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política para el Uso de Medios Removibles	Mayo de 2018	

Tabla 14. Formato de Aprobación Política para el Uso de Medios Removibles
Fuente: http://www.informationshield.com

1.2.6 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

Políticas de Seguridad de la Información					
Política de Escritorio y Pantalla Limpia					
Política	IS-05	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 15. Formato de Cabecera Política de Escritorio y Pantalla Limpia
Fuente: http://www.informationshield.com

PROPÓSITO:

Establecer los lineamientos generales para que los funcionarios, contratistas y proveedores de HECC COURRIER conserven el puesto del trabajo y pantalla del equipo de cómputo limpio de documentos, archivos o dispositivos de almacenamiento removibles.

ALCANCE:

Los funcionarios o empleados y proveedores de HECC COURRIER que tengan acceso a la información tanto en formato físico como digital deberán cumplir con la política aquí descrita.

DETALLE:

HECC COURRIER cuenta con una política de escritorio limpio / pantalla limpia como mecanismo para reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante y fuera de las horas laborales normales. Estas políticas se rigen por los requisitos legales, contractuales y las directrices de manejo de la información**.**

1. EQUIPOS DE USUARIOS DESATENDIDOS

Todo empleado de HECC COURRIER debe garantizar que a los equipos desatendidos se les da protección apropiada, para ello cada empleado debe:

- ✓ Realizar un registro de cierre de la sesión iniciada en aplicaciones y herramientas de transferencia de información (es decir, no sólo apagar el interruptor de la pantalla).
- ✓ Al finalizar la jornada laboral, cerrar todas las sesiones o accesos disponibles, en caso de no ser posible asegurarse de proteger el equipo con contraseña.

2. POLITICA DE ESCRITORIO LIMPIO

Todo empleado debe mantener su puesto de trabajo libre de información confidencial, contenida en medios de almacenamiento como documentos, cuadernos, USB…, garantizando que en caso de contar con ellos, se toman las medidas para guardarlos en lugares seguros durante periodos de recesos largos, por ejemplo al finalizar la jornada laboral, asimismo cuando el empleado se encuentre fuera de la oficina o en áreas de atención al público debe tener especial cuidado con el manejo que le dé a la información a su cargo.

Los empleados no deben tener documentos con información laboral (archivos excel, word, pdf, bloc de notas), accesos directos ni documentación de los sistemas de gestión en el escritorio del equipo. La información laboral (registros) se debe guardar en la unidad D:\HECC y en las unidades de almacenamiento corporativos (por ejemplo, carpetas compartidas), según estándares específicos de cada proceso. Para la mayoría aplica estrictamente el uso de carpetas compartidas y no en el equipo individual.

El escritorio del equipo debe estar limpio y únicamente debe contener los iconos de los programas instalados por Infraestructura Tecnológica durante la configuración. Esto incluye vaciar diariamente la papelera de reciclaje y el acceso/carpeta de documentos recientes

3. POLÍTICA DE PANTALLA LIMPIA

Cuando un empleado se ausente del puesto de trabajo, debe asegurarse de mantener el equipo salvaguardado para evitar la posibilidad de suplantación y acceso no autorizado a información, herramientas y usuarios a su cargo, para ello es obligatorio que cada empleado cierre las sesiones de usuario en todas las estaciones de trabajo y proteja el equipo con un mecanismo de bloqueo de pantalla controlado por una contraseña, lo cual funciona con el siguiente comando:

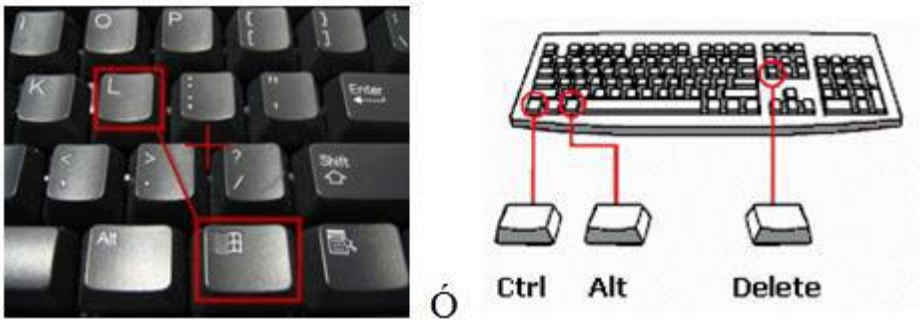


Ilustración 1. Teclas de Bloqueo
Fuente: http://www.seas.ucla.edu/security/lock_session.html

Esto se debe cumplir siempre que el equipo no pueda ser custodiado por el empleado mismo. El área de Sistemas controla la política de bloqueo de seguridad de Windows al detectar 3 minutos de inactividad.

RESPONSABILIDADES

- ✓ Los funcionarios o empleados de HECC COURRIER serán los responsables del buen uso de la información tanto física como lógica, y del cumplimiento de los lineamientos determinados en esta política.
- ✓ Los equipos de cómputo y lugares de trabajo podrán ser revisados y auditados por las áreas de control que determine HECC COURRIER, a fin de validar el cumplimiento de la presente política.
- ✓ El área de Sistemas será la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso de tiempo determinado.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de Escritorio y Pantalla Limpia	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Angel Leguizamón	Política de Escritorio y Pantalla Limpia	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Escritorio y Pantalla Limpia	Mayo de 2018	

Tabla 16. Formato de Aprobación Política de Escritorio y Pantalla Limpia
Fuente: http://www.informationshield.com

1.2.7 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Políticas de Seguridad de la Información					
Política de Seguridad Física y del Entorno					
Política	IS-03	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 17. Formato de Cabecera Política de Seguridad Física y del Entorno
Fuente: http://www.informationshield.com

PROPÓSITO:

Evitar el daño, interferencias y el acceso no autorizado a la información o activos pertenecientes a la organización.

ALCANCE:

Aplica cuando un empleado, visitante, proveedor o una parte interesada requiere ingresar a las instalaciones de HECC COURRIER. Los responsables de cumplimiento son todos los empleados de HECC COURRIER.

DETALLE:

Todo empleado de HECC COURRIER debe cumplir las siguientes instrucciones:

- En caso de que necesite quedarse hasta tarde y ser la última persona en salir de HECC COURRIER debe solicitar la autorización de su jefe inmediato para indicarle al vigilante del conjunto de bodegas donde se encuentra HECC COURRIER que puede habilitar la alarma y cerrar las puertas bajo llave una vez termine las labores que se estén desarrollando.
- Es prohibido estar en las instalaciones de HECC COURRIER después de las 8 de la noche sin autorización o saltar o vulnerar la seguridad física de HECC COURRIER. Esto se considera una falta grave y se sanciona según reglamento interno de trabajo.
- Es prohibido ingresar a un área diferente a la asignada para su cargo, cuando no hay nadie. Esto significa que nadie ajeno a las áreas puede estar allí cuando no hay ningún integrante del área, exceptuando servicios generales y algún integrante del área de sistemas (si están atendiendo una solicitud).
- Evitar el acceso no autorizado, el robo o la puesta en peligro de la información
- Resguardar los medios que contienen información, así como los servicios de procesamiento de la misma.
- Informar cualquier evento sospechoso o fuera de lo común.

Los controles de seguridad física con los que debe contar HECC COURRIER son:

Sistema de Control de Acceso por Tarjetas de Aproximación

- **Funcionarios o Empleados:**

Cada empleado al ingresar a HECC COURRIER recibe dos tarjetas de aproximación: una para el acceso al conjunto de bodegas y una para el acceso a las oficinas las cuales son de uso personal e intransferible. Para el uso y cuidado de las tarjetas es importante tener en cuenta:

a) El sistema cuenta con un sistema de bloqueo (antipassback) que se encuentra activo en todas las puertas, de modo que los empleados que no marquen su ingreso no podrán salir de las oficinas de HECC COURRIER y viceversa. Es obligación de todos los empleados pasar su tarjeta por todos los lectores.
b) En caso de olvido: si el empleado se presenta a trabajar y no cuenta con la tarjeta de ingreso al conjunto, se debe registrar en la portería del conjunto, pedir autorización de ingreso y portar un carnet de visitante y al terminar la jornada laboral debe regresarlo. Si la tarjeta que olvidó es la de acceso a la oficina, debe registrarse en la recepción de HECC COURRIER, firmando el control de tarjetas de préstamo. Esta tarjeta no debe permanecer en poder del empleado solicitante por más de 3 días hábiles, si pasados los tres días el empleado no regresa la tarjeta de acceso se debe informar al Área de Sistemas.
c) Cuando el empleado requiere tramitar el préstamo de tarjeta y no se encuentra ningún funcionario encargado de recepción, debe esperar en la recepción de HECC COURRIER hasta que le sea asignada una tarjeta de préstamo. Queda rotundamente prohibido que otro empleado ingrese a la persona, esto da lugar a un llamado de atención para las dos personas. De igual manera está prohibido que un empleado de HECC COURRIER tome tarjetas sin dejar el registro en las plantillas correspondientes, esto da lugar a un llamado de atención.
d) En caso de pérdida de la tarjeta de acceso, es obligatorio informar de manera inmediata al departamento de Gestión Humana, para que este a su vez le informe al Área de Sistemas para su desactivación y reposición. El empleado debe pagar a HECC COURRIER el costo de reposición de cada tarjeta (valor de veinte mil pesos $20.000 para la tarjeta de acceso a la oficina y de treinta mil pesos $30.000 para la tarjeta de acceso al conjunto) este pago se debe realizar por descuento de nómina en la siguiente quincena o mensualidad en una sola cuota.

- **Visitantes**
  a) Todo visitante sin excepción alguna debe anunciarse en la portería del conjunto donde se encuentra HECC COURRIER. En la portería del conjunto se les entrega tarjeta de visitante.
  b) Cuando el encargado de recepción entrega la tarjeta al visitante, debe informarle que tiene la obligación de marcar su acceso por cada uno de los lectores de tarjetas que encuentre durante el trayecto hacía el área que se dirige.

Carné de Identificación Para Empleados Y Para Visitantes

Es responsabilidad del departamento de Gestión Humana asegurar la entrega del carné de identificación a todos los empleados de HECC COURRIER el cual deben portar en un lugar visible durante el tiempo que se encuentre en las instalaciones de la empresa o del cliente. En caso de pérdida, el valor aproximado del carné de identificación es de $5.000.

Es deber del responsable de la recepción, asignar un carné de identificación a los visitantes dejando evidencia en el Registro de seguridad para visitantes, se debe informar al visitante que es obligatorio portar el carné de manera visible**.**

Control de Visitantes

- **Actividades para realizar antes, durante y después de la visita.**

Para realizar antes de la visita:

a) Es obligatorio que las personas encargadas de la recepción cumplan los horarios para evitar que lleguen visitas a HECC COURRIER y no haya quien las reciba.
b) Como generalmente las visitas son planeadas, todos los empleados de HECC COURRIER están obligados a cumplir las citas con puntualidad, para evitar inconvenientes en el control de ingreso o inconformidades. de los visitantes (especialmente los clientes).
c) En caso de que la persona de recepción no reciba indicaciones cuando hay imprevistos, debe contactar al jefe inmediato de la persona encargada de la visita para solicitar información al respecto. La persona encargada de recepción solo puede llamar al celular a las personas que autoricen incluir su número de contacto en el directorio de la recepción.

Para realizar durante la visita:

- Solicitar al visitante un documento de identificación diferente a la cédula de ciudadanía (preferiblemente el carné empresarial para visitas de clientes y proveedores), en lo posible que tenga foto y número de identificación para guardarlo durante la estadía del visitante en HECC COURRIER y entregarle a cambio la tarjeta de acceso y el carné de identificación.
- Informar la llegada de la visita al empleado de HECC COURRIER para que lo acompañe hasta el lugar en el cual será atendido.
- Si el visitante requiere acceso a las áreas de seguridad máxima, previamente debe estar diligenciada la aprobación mediante la plantilla de correo electrónico Aprobación ingreso visitantes a áreas restringidas. Una vez se encuentre la plantilla diligenciada con las aprobaciones requeridas, la persona responsable de la recepción es responsable de integrar las aprobaciones y guardar el formato en la ruta correspondiente.
- Entregar al visitante el registro de seguridad para visitante que se debe diligenciar antes de iniciar la visita.
- El Empleado de HECC COURRIER debe acompañar al visitante a la recepción de la organización en cuanto se finalice la visita.

Para realizar al finalizar la visita:

- Reclamar al visitante el carné y la tarjeta de visitante asignada.
- En caso de pérdida de la tarjeta de acceso, el encargado de recepción debe comunicarse con el área de sistemas para bloquearla inmediatamente y a gestión humana para gestionar con el visitante el pago de la tarjeta perdida.
- Regresar el documento de identificación al visitante.

Controles de acceso según el tipo de visitante

- **Proveedores**
  a) Proveedores de Suministros, mensajeros y domicilios: se debe tener en cuenta que los suministros y mercancía se dejan en el área de la recepción y el empleado encargado, debe retirarlos y almacenarlos en el lugar destinado para ello.
  b) Proveedores de Mantenimiento: Mantenimiento realizado durante la jornada laboral: además de cumplir lo establecido el proveedor debe estar acompañado permanentemente por el empleado que solicita el servicio de mantenimiento, en caso de no ser necesario, se debe solicitar a la alta gerencia autorización para que el proveedor pueda realizar las actividades sin acompañamiento y debe seguir las actividades.
  c) Proveedores de construcción: Cuando se realice una obra civil en HECC COURRIER, la persona encargada debe primero realizar un análisis previo del tipo de proveedor que ejecutará la obra. Segundo analizar los riesgos asociados al tipo de información que se maneja en dicho lugar. Y por último determinar si el proveedor contará con compañía permanente o tendrá un supervisor de obra encargado de manipular los controles de seguridad físicos o se le asignaran llaves, claves y demás. Dicho manejo debe quedar aprobado por la alta gerencia Información por correo electrónico.

- **Clientes**

Además de cumplir lo establecido se debe:

  a) Solicitar/apartar con anticipación la sala de juntas y planear los demás requerimientos de tipo logístico y técnico requeridos.
  b) En cualquier caso, siempre el cliente debe estar acompañado del responsable de la organización.

Restricciones de Acceso Según el Tipo de Área

HECC COURRIER está conformada por diferentes áreas donde el acceso es restringido y controlado por perímetros de seguridad físicos como paredes, lectores de tarjetas de aproximación, puertas, cámaras, recepción y directrices documentadas de obligatorio cumplimiento, que buscan garantizar la integridad, disponibilidad y confidencialidad de la información según los servicios de procesamiento y el tipo de información que se maneja en cada una. Las áreas de HECC COURRIER según nivel de acceso son las siguientes:

- ✓ Áreas de seguridad máxima.
- ✓ Áreas de carga, despacho y acceso público.

A continuación, se describen las políticas que rigen el acceso a las áreas de HECC COURRIER y se dictan las restricciones de acceso.

1. Áreas de seguridad máxima:

   Áreas en las que opera la modalidad de Operaciones y se administran los servidores productivos y de respaldo utilizados en las modalidades de negocio de correspondencia:

   - ✓ Operaciones: Cuando se trata del ingreso de un visitante a esta área, el responsable de la visita debe indicar desde la puerta quién va a ingresar y con qué motivo y luego si hacer pasar al visitante. Si la visita implica que los integrantes de Operaciones presten atención o participen de alguna manera (por ejemplo, para una presentación de nuevos empleados, pausas activas, etc.), todos los empleados deben bloquear sus equipos (tecla Windows + L) mientras la visita se retira del departamento. Para visitas prolongadas que impliquen obligatoriamente atención en sitio se debe asegurar que el visitante permanezca en el puesto autorizado y no realice desplazamientos dentro del área. Esto aplica particularmente para auditorias. Para visitas prolongadas de un cliente, prospecto o proveedor se debe realizar atención en sala de juntas.
   - ✓ Área de Sistemas: Las visitas al centro de donde HECC COURRIER tiene sus servidores productivos solo son permitidas para los empleados y clientes de la organización y se debe: Enviar un correo electrónico con la solicitud de la visita a la alta gerencia para su debida autorización. Una vez se cuenta con la aprobación, enviar a sistemas: el nombre, número de cédula, ARL, y EPS, de los visitantes programados, esta visita se debe coordinar entre 15-20 días antes. Solicitar una visita guiada, si la visita requiere el conocimiento de los sistemas de seguridad física, ambiental y los respaldos de los servicios contratados por HECC COURRIER.

   Los empleados ajenos a las áreas de seguridad máxima con autorización de acceso, solo podrán ingresar con acompañamiento del personal del área respectiva. Si un empleado de HECC COURRIER requiere ingresar a las áreas de máxima seguridad, debe enviar un correo de aprobación ingreso visitante a áreas restringidas. Una vez se encuentre el correo diligenciado con las aprobaciones requeridas la asistente de recepción le entrega la tarjeta de acceso que tiene permisos de ingreso.

   Si un empleado requiere ingresar al área de Sistemas momentáneamente por inquietudes o por solicitudes de cambios o de servicios, debe hacerlo en compañía del personal perteneciente al área y bajo ninguna circunstancia puede permanecer solo al interior del área. El ingreso de los

empleados que no tienen habilitada la tarjeta de acceso a esta área, se controla por medio de las cámaras de seguridad.

2. Áreas de carga, despacho y acceso público

   Área designada para la recepción de visitantes y para la recepción de mensajería/paquetes:

   - ✓ Recepción de HECC COURRIER: áreas de carga, despacho y acceso público. Para recibir visitantes y proveedores no conocidos.

RESPONSABILIDADES

El responsable de la seguridad de la información: Este asumirá y dirigirá las políticas a seguir en la protección de los equipos, del mantenimiento y control de acceso etc. Se encargará de separar las áreas (Para servidores se creará un área restringida que tendrá un tratamiento especial). Se responsabilizará de aceptar todas las políticas establecidas por el responsable de la seguridad y revisará el cumplimiento de las mismas.

Como se mencionó antes también los responsables son todos los empleados de HECC COURRIER.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de Seguridad Física y del Entorno	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Angel Leguizamón	Política de Seguridad Física y del Entorno	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Seguridad Física y del Entorno	Mayo de 2018	

Tabla 18. Formato de Aprobación Política de Seguridad Física y del Entorno
Fuente: http://www.informationshield.com

1.2.8 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

Políticas de Seguridad de la Información					
Política de Controles Criptográficos					
Política	IS-11	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 19. Formato de Cabecera Política de Controles Criptográficos
Fuente: http://www.informationshield.com

PROPÓSITO:

Establecer las normas para proteger la confidencialidad, integridad y disponibilidad de la información, mediante el uso y aplicación de técnicas en la organización. Tener segura la información clasificada, con el uso de la herramienta de cifrado para transferencias de archivos con esta clasificación, por medio de los sistemas de información y comunicaciones.

ALCANCE:

La presente política es aplicable a todos los empleados de Hecc Courrier que mantengan contacto directo con la información confidencial o privada, para el uso de algoritmos criptográficos como herramientas de control, protección de la confidencialidad e integridad de la información.

DETALLE:

Las técnicas criptográficas deben ser utilizadas en caso de los controles actuales de organización no satisfagan una adecuada protección de la información. El Área de Sistemas debe verificar los sistemas o aplicaciones que realicen y/o permitan la transmisión de información confidencial o privada, lo realicen mediante herramientas de cifrado de datos.

El Área de Sistemas proveerá la herramienta de cifrado de datos a los usuarios, previa solicitud formal. La asignación de la clave para el cifrado de la información en la herramienta, debe ser establecida por el usuario que administra dicha información, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable. Los controles criptográficos se usarán en los siguientes casos:

- ✓ En la protección de claves de acceso a sistemas, datos y servicios.
- ✓ Para la transmisión de información Confidencial o Privada, fuera de la Entidad.
- ✓ En la protección de la información a resguardar, cuando así lo establezca la organización.
- ✓ Si los datos de un medio de almacenamiento se encuentran cifrados incluso en modo de respaldo, las llaves de cifrado deben ser almacenadas en otro medio de almacenamiento separado
- ✓ Si se utilizan técnicas criptográficas, la información protegida debe ser transferida por un medio distinto al utilizado para transferir las llaves criptográficas.
- ✓ Estudiar la posibilidad de implementar certificados de clave pública.
- ✓ Los procesos de intercambio de información internos que requieran garantizar la identificación plena de los usuarios, así como la integridad y confidencialidad de la información que se utilizan, deben estar soportados por el uso de herramientas de cifrado.

Para establecer el sistema de cifrado, se tienen en cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente. Para el cifrado de información se utilizarán algoritmos de cifrado simétrico como:

- ✓ AES de longitud 128/192/256
- ✓ RC4 de 128 bits
- ✓ RC2 de 128 bits

La organización no establece una directriz de ciclo de vida de llaves criptográficas, toda vez que, la asignación de la clave para el cifrado de la información en la herramienta, la establece el usuario que genera o administra la información a cifrar, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.

RESPONSABILIDADES

La solicitud de acceso o actualización al sistema o claves de cifrado se debe efectuar de manera formal al área de Sistemas. Aquellas personas autorizadas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las claves criptográficas, así como de la información a la cual se le haya aplicado algún proceso de cifrado. En el mismo modo, la información cifrada o descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de una eliminación segura.

El área de operaciones que es el área que maneja más información confidencial o privada será la encargada de la responsabilidad de realizar la solicitud en la utilización de las herramientas de cifrado al área de sistemas.

APROBACIÓN

Elaborado	**Título**	**Fecha**	**Firma**
Autores del documento	Política de Controles Criptográficos	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política de Controles Criptográficos	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Controles Criptográficos	Mayo de 2018	

Tabla 20. Formato de Aprobación Política de Controles Criptográficos
Fuente: http://www.informationshield.com

1.2.9 POLÍTICAS CONTRA CODIGO MALICIOSO

Políticas de Seguridad de la Información					
Política Contra Código Malicioso					
Política	IS-10	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 21. Formato de Cabecera Política Contra Código Malicioso
Fuente: http://www.informationshield.com

PROPÓSITO:

La protección de la confidencialidad, autenticidad o integridad de la información de HECC COURRIER a través de controles contra código malicioso.

ALCANCE:

Las políticas contra código malicioso se aplicarán para certificar la confidencialidad, integridad y/o autenticidad en el tratamiento de la información de HECC COURRIER.

DETALLE:

1. **Reglas para el uso de equipos y dispositivos de red**

   A cada empleado se le asigna un equipo de trabajo que es para uso laboral exclusivamente. El equipo es configurado por el área de Sistemas y como es un elemento de uso exclusivo de la compañía sólo los miembros del departamento de Infraestructura tecnológica pueden realizar modificaciones, por lo tanto, para los empleados de HECC COURRIER no es permitido.

   - ✓ Modificar o vulnerar los permisos de configuración de los equipos.
   - ✓ Violar los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución, descarga, e instalación de software sin la licencia "pirata" o sin permiso de uso adquirido por HECC COURRIER.
   - ✓ Sacar los equipos, la información o el software de las instalaciones de HECC COURRIER sin el debido proceso de autorización.
   - ✓ Retirar el sello Azul de seguridad que protege las partes internas de los activos de HECC COURRIER, este sello solo debe ser retirado por un empleado del área de Sistemas. Las etiquetas de identificación de activos no deben ser manipuladas, intercambiadas o destruidas por empleados que no pertenezcan al área de HECC COURRIER.
   - ✓ Conectar dispositivos a la red (Switch, Routers, etc.) que no sean propiedad de HECC COURRIER, o que no estén debidamente autorizados (por correo electrónico) para su uso.

2. **Control de Virus y Códigos Malicioso**

   El área de Sistemas cuenta con software de detección, prevención y esquemas de recuperación contra código malicioso que es un programa informático instalado en el equipo sin que el usuario o infraestructura lo sepan, se transmite cuando un usuario navega en sitios web infectados o cuando se instalan programas mediante engaños; algunos de los objetivos que persiguen estos programas es:

   - ✓ Dañar los sistemas internos del equipo, borrar datos o deteriora el

rendimiento (equipos lentos).
- ✓ Usar el equipo para transmitir virus y mensajes de correo electrónico no deseados.
- ✓ Robar información personal usuarios claves y datos con el fin de robar la identidad (dichos programas se denominan "spyware").

Los códigos maliciosos pueden tomar diversas formas, por ejemplo:

SCRIPTS	Intentan ejecutarse en tu equipo cuando visitas un sitio web infectado. La mayoría de los exploradores modernos te advertirá que un sitio web desea ejecutar un script cuando esto ocurra. Por ejemplo, algunos sitios web intentarán instalar un pequeño archivo en tu equipo para que recuerde tu información en la próxima visita (dicho archivo se denomina "cookie").
GUSANOS	Son tipos de virus que se envían a través de mensajes de correo electrónico y también, a través de mensajes instantáneos. Con frecuencia, están ocultos en mensajes de correo electrónico y mensajes instantáneos como archivos adjuntos.
VIRUS	Estos programas se distribuyen a través de vínculos de red entre equipos. Para funcionar, se instalan en el equipo infectado y le dan instrucciones, generalmente para deteriorar el rendimiento del equipo o dañarlo y también para distribuirse en la mayor cantidad de equipos posible.
TROYANOS	Estas descargas maliciosas incluyen códigos ocultos en otros programas que el usuario realmente desea descargar. Con frecuencia música, actualizaciones y elementos emergentes.

Tabla 22. Tipos de Códigos Maliciosos
Fuente: Los Autores

Por lo anterior, ningún usuario podría realizar cambios no autorizados, los cambios solo son realizados por personal del área de Sistemas, que además se encarga de verificar la Instalación y actualización regular del software de detección y reparación de códigos maliciosos para explorar los computadores. Es importante recordar que:

- ✓ Cada equipo de escritorio y servidor tiene instalado un antivirus (Symantec) el cual se actualiza de manera automática cada vez que se encuentran nuevas definiciones de virus, esto se realiza a través de la consola de antivirus la cual está configurada para que periódicamente descargue las actualizaciones.
- ✓ El antivirus instalado en los clientes tiene la propiedad de escanear en tiempo real los archivos provenientes de medios ópticos y electrónicos.
- ✓ El antivirus tiene habilitado la propiedad de realizar un diagnóstico de las descargas para detectar riesgos en archivos descargados

según reputación. La reputación del archivo indica cuán potencialmente dañino o no es un archivo.

- ✓ El antivirus cuenta con la opción de análisis de los correos electrónicos tanto de Internet como para el Outlook, esta opción, la cual se encuentra habilitada escanea todos los archivos adjuntos y en caso de que el archivo venga comprimido, puede revisar hasta un nivel definido por el administrador, en este caso está configurado hasta el tercer nivel.
- ✓ También se cuenta con un firewall el cual cuenta con un antivirus perimetral para las descargas desde la red local hacia internet a través de los protocolos: HTTP, HTTPS, FTP, SMTP, SMTPS, IMAP, IMAPS, IM. (Estos son los protocolos sobre los cuales se realiza este control).

¿Cuál es la responsabilidad de los empleados frente al riesgo asociado a los códigos maliciosos?

El área de Sistemas recibe información de grupos de interés que informan sobre vulnerabilidades que le permiten tomar acciones, además se encarga de instalar, controlar y mantener el software de detección y reparación de códigos maliciosos y realizar verificaciones periódicas programadas como mantenimientos; sin embargo la mejor manera de evitar los códigos maliciosos de todo tipo es mantener el antivirus actualizado, todos los equipos de HECC COURRIER tienen el firewall habilitado y cuentan con un bloqueo de páginas definidas como poco seguras o no productivas; sin embargo el usuario debe visitar sitios web seguros y legítimos. Los scripts, como las cookies, no se pueden ejecutar o descargar sin un permiso expreso. Se debe cumplir lo establecido en la política de software para evitar descargar software maligno y reportar las debilidades de seguridad detectadas que puedan poner en riesgo la continuidad de las operaciones.

3. Política para Uso de Software

El área de Sistemas, es el encargado de la adquisición de software conforme a las necesidades de seguridad y de negocio detectadas; respetando, la normatividad de derechos de autor y propiedad intelectual vigente. Todo software que no sea adquirido mediante este proceso se considera software no autorizado y se prohíbe su uso, en caso de requerir software “gratuito”, dicho software debe ser probado y aprobado por el departamento de Infraestructura tecnológica, quienes se encargarán de garantizar que su descarga y uso no generará vulnerabilidades de seguridad de la información, o potenciara riesgos, daños o errores en los sistemas, además de validar la necesidad de su uso; está prohibido el uso de software no aprobado por el área de Sistemas. En conformidad con lo anterior, el área de Sistemas lleva a cabo revisiones regulares del software y del contenido de datos de los sistemas y herramientas de negocio.

En HECC COURRIER, la instalación de software se encuentra controlada

por el área de Sistemas, cuando un empleado requiera instalar software de uso gratuito empresarial, deberá utilizar enviar una solicitud de cambios y o servicios, esta instalación deberá ser autorizada por el director del área del solicitante y por el área de Sistemas. El área de Sistemas autorizará esta instalación solo si el software es libre para empresas como HECC COURRIER. En caso de requerir software con costo, se deberá enviar la solicitud con aprobación de la Alta Gerencia para realizar el proceso de compras.

Los usuarios de dominio de los empleados no son administradores, en caso de existir razones de negocio que requiera estos privilegios, se deberá contar con la autorización de la alta Gerencia; estos usuarios serán sometidos a auditorias periódicas por parte del área de Sistemas.

RESPONSABILIDADES

- ✓ Los empleados, tendrán la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales del sistema o los posibles riesgos asociados al cifrado de la información.

- ✓ Los responsables de los sistemas serán los encargados de establecer los controles para asegurar el sistema, y de restringir su acceso a los empleados. Así mismo tendrán una copia de respaldo que será guardada en sitio seguro por la persona delegada para tal función, y quien procederá a facilitarla en caso de que la llave sea requerida.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política Contra Código Malicioso	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Angel Leguizamón	Política Contra Código Malicioso	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política Contra Código Malicioso	Mayo de 2018	

Tabla 23. Formato de Aprobación Política contra Código Malicioso
Fuente: http://www.informationshield.com

1.2.10 POLÍTICA DE ALMACENAMIENTO Y RESPALDO

Políticas de Seguridad de la Información					
Política de Almacenamiento y Respaldo					
Política	IS-06	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 24. Formato de Cabecera Política de Almacenamiento y Respaldo
Fuente: http://www.informationshield.com

PROPÓSITO:

Definir los lineamientos y directrices para la generación, administración y resguardo de las copias de respaldo, tiendo la finalidad de asegurar la disponibilidad e integridad de la información.

ALCANCE:

La política de almacenamiento y respaldo debe ser de obligatorio cumplimiento por parte de los empleados que realicen, administren y custodien las copias de respaldo definidas por la HECC COURRIER, reduciendo ante todo el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad del negocio.

DETALLE:

HECC COURRIER establece los procedimientos de rutina suficientes para garantizar la continuidad de las operaciones de sus servicios ofrecidos, bajo los pilares de integridad, confidencialidad y disponibilidad de la información, acorde con los tiempos de respuesta establecidos, enmarcados en la mejora continua. La información requerida en el desarrollo de las operaciones orientadas al cumplimiento de los objetivos estratégicos HECC COURRIER, deberá tratarse conforme a los lineamientos legales, técnicos y administrativos determinados a los a los niveles de clasificación de la información.

Los tiempos de salvaguardar de las copias de respaldo de HECC COURRIER se definirán según los requerimientos técnicos, administrativos y jurídicos, y se determinarán por parte de la entidad los recursos requeridos para acceso y validación de la información contenida durante los tiempos previstos.

La solicitud de respaldo deberá presentarse formalmente al responsable de las copias de respaldo, determinando las necesidades, la información sujeta al respaldo, periodos, niveles de clasificación de la información y el tiempo de retención de las copias. Así mismo, se realizarán las respectivas pruebas de funcionamiento conforme a los propósitos para los cuales han sido recaudadas.

Los funcionarios del área de Sistemas encargados de las copias de respaldo, velarán para que, durante su transporte y custodia, la misma no sea manipulada por personas no autorizadas.

Las copias de respaldo deberán ser almacenadas en lugares que tengan los debidos controles de seguridad físicos y tecnológicos, esto es, que permitan limitar
el acceso sólo a las personas autorizadas y garanticen la disponibilidad de la información. También, deberán registrarse todas las actividades desarrolladas frente al tratamiento y manipulación de las copias para guardar la trazabilidad.

Cuando caduca el tiempo requerido de almacenamiento de las copias de respaldo, se deberá proceder a su destrucción o eliminación, asegurando que la información contenida no sea accedida por personas no autorizadas. Las

actividades realizadas deberán ser registradas para su posterior consulta.

Respaldos de Información

1. **Respaldos de Información de los Directores**

   Estos respaldos se realizan a los equipos de las direcciones de las distintas áreas. Para el caso de las direcciones que usen portátiles para sus labores diarias y que sean propiedad de HECC COURRIER y que en ocasiones no se encuentran en las instalaciones de HECC COURRIER, deberán coordinar con infraestructura tecnológica para facilitar el acceso al equipo y poder contar con el respaldo correspondiente.

   - ✓ La copia de respaldo para las direcciones es de tipo full manualmente a un disco duro externo el cual es guardado en la caja fuerte del área de Sistemas, realizándolo a los archivos contenidos dentro del directorio “D:\SQL”, cuando en dicha ruta solo se tenga el archivo .pst no es necesario realizar el respaldo, ya que el .pst se encuentra en la nube debido al servicio de Office365, en dicho caso las Direcciones que consideren que no es necesario realizar el respaldo envían un correo a infraestructura tecnológica informado la no la realización del respaldo
   - ✓ Los respaldos a las direcciones se realizan mensualmente. Se deben ejecutar manualmente la segunda semana de cada mes.

2. **Respaldo de Información para Empleados Activos**

   Estos respaldos se ejecutan a empleados activos que no tengan rol de dirección de las distintas áreas. Para el caso de empleados activos que usen portátiles para sus labores diarias y que en ocasiones no se encuentran en las instalaciones de HECC COURRIER, infraestructura tecnológica les enviará un correo electrónico confirmándole el recurso compartido en donde deben alojar su respectivo respaldo, para que sean los empleados los responsables de cumplir con este requerimiento.

   - ✓ Los directorios y archivos; excepto el .pst; el cual se encuentra en la nube Office365, que se respaldan a los empleados activos de las diferentes áreas de la compañía.
   - ✓ El tipo de respaldo que el área de sistemas utiliza para los respaldos de empleados activos es full, es decir, se copia toda la información contenida en el directorio mencionado en el punto anterior.
   - ✓ Este tipo de respaldo se realizan directamente en el equipo del empleado de manera manual, llevando a cabo una copia de la información a respaldar en un disco duro externo el cual es guardado en la caja fuerte del área de Sistemas.
   - ✓ Los respaldos realizados a los empleados activos, tienen una periodicidad semestral.
   - ✓ La retención de los respaldos en medio magnético de los empleados activos en HECC COURRIER se encuentra entre 3 a 5

años.

- ✓ El formato con el cual quedan los respaldos de los archivos y directorios de los empleados activos es el mismo de origen, dado que no se utiliza ninguna herramienta para su compresión.

3. Respaldo de Información Para Empleados Retirados

Estos respaldos se ejecutan a empleados retirados de la compañía

- ✓ A cada empleado que se retira de la compañía, se le efectúa la extracción de la información contenida en el directorio D:\HECC e igualmente del correo electrónico.
- ✓ El tipo de respaldo que el área de sistemas utiliza para los respaldos de empleados activos es full, es decir, se copia toda la información contenida en el directorio mencionado en el punto anterior.
- ✓ Este tipo de respaldo se realizan directamente en el equipo del empleado, llevando a cabo una copia de la información a respaldar en un medio extraíble, para luego quemarlo en un medio magnético y custodiarlo en la caja fuerte perteneciente al área de Sistemas.
- ✓ Los respaldos realizados a los empleados retirados, se llevan cabo cada vez que un empleado termina su contrato laboral con HECC COURRIER.
- ✓ La retención de los respaldos en medio magnético de los empleados activos en HECC COURRIER es de 3 años.
- ✓ El formato con el cual quedan los respaldos de los archivos y directorios de los empleados retirados es el mismo de origen, dado que no se utiliza ninguna herramienta para su compresión.

Grabado, Registro Y Custodia De Medios Magnéticos

Una vez se hayan realizado los respaldos anteriormente descritos y se encuentran en el repositorio de respaldos, se procede al registro, grabado en un medio diferente al servidor de repositorio de respaldos con el fin de liberar espacio y por ultimo enviar los medios generados a custodia. Generalmente estos medios son CD, DVD O BLUE RAY**.**

1. Etiquetado de Medios

El medio creado, debe ser etiquetado con los siguientes datos:

DESCRIPCIÓN CONTENIDO	Se describe el contenido de la información que se está quemando
FECHA	Mes y año de la realización del respaldo
SERVIDOR, IP O CONTENIDO	Origen del backup

Tabla 25. Tipos de Etiquetado de Medios
Fuente: Los Autores

2. Custodia de Medios

El proceso de almacenamiento para los medios de información se tiene que contratar proveedor se sugiere (Thomas) quienes deberán garantizar a HECC COURRIER la protección y seguridad de los medios entregados para su custodia. Se tiene establecida una frecuencia mensual para recoger los nuevos medios generados.

Previa a la entrega de los medios al proveedor se diligencia Acta de entrega de copias para custodia *(formato de Word)* la cual es la evidencia de las copias entregadas al proveedor para custodia. Así mismo, se posee 4 tulas (enumeradas del 1 al 4) que son custodiadas, las cuales son usadas cuando no se cuenta con espacio disponible con el proveedor.

RESPONSABILIDADES

- Los empleados responsables de la infraestructura, sistemas de información y Bases de datos requeridos para la operación de HECC COURRIER, deberán generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido en la presente política.

- Los encargados de las copias de respaldo deben velar porque la información sea almacenada conforme a los lineamientos establecidos, es decir, de forma controlada y según las necesidades de HECC COURRIER. Así mismo deberán realizar una prueba periódica de las copias con el fin validar el correcto funcionamiento y la efectiva restauración.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de Almacenamiento y Respaldo	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política de Almacenamiento y Respaldo	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Almacenamiento y Respaldo	Mayo de 2018	

Tabla 26. Formato de Aprobación Política de Almacenamiento y Respaldo
Fuente: http://www.informationshield.com

1.2.11 POLÍTICA DE CONTROL Y GESTIÓN DE LOS SERVICIOS DE RED

Políticas de Seguridad de la Información					
Política de Control y Gestión de los Servicios de Red					
Política	IS-09	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 27. Formato de Cabecera Política de Control y Gestión de los Servicios de Red
Fuente: http://www.informationshield.com

PROPÓSITO:

Evitar el acceso no autorizado a los servicios de red, ejerciendo un control sobre los perfiles de acceso suministrados en HECC COURRIER, de modo que no comprometan la seguridad.

ALCANCE:

La presente política deberá ser adoptada por todos los empleados de HECC COURRIER que realicen uso de la red de información en cumplimiento de sus funciones.

DETALLE:

Los usuarios de servicios de red de HECC COURRIER tienen acceso a los servicios necesarios para la ejecución de sus actividades bajo entornos seguros, se indicarán las restricciones de acceso de red generadas, que, apoyados en herramientas de control y aseguramiento de las redes, permiten mitigar la probabilidad de generación de incidentes de seguridad de la información. El proceso de autorización para el uso de los servicios de red, para visitantes y terceros, se parametriza, conforme a la política de Seguridad física y del Entorno de HECC COURRIER.

1. **Segmentación de la Red**

   Uno de los mecanismos utilizados por HECC COURRIER para controlar la red, es la subdivisión de red interna en dominios, cada dominio se encuentra protegido con políticas de acceso y control de contenido específico, fundamentado en la política de control de acceso, en la clasificación de la información que se realiza.
   En HECC COURRIER existen los siguientes segmentos de red internos en la oficina principal, está segmentación se realizó por grupos de trabajo unidos de la siguiente manera:

   - Comercial
   - Recursos Humanos
   - Administrativa y Financiera

- Contable
- Sistemas
- Gerencia

Se debe realizar la segmentación (VLAN) configurable en los Switches, siendo el Switch principal y administrador, el Switch JUNIPER EX2200.

2. Control de Servicios de Red

Buscando prevenir y controlar el acceso que tienen los empleados y visitantes de HECC COURRIER a la red; el área de Sistemas, realiza un estricto control de contenido en Internet, agrupando perfiles de accesos comunes en los que se administran los permisos de acceso a las páginas necesarias para desempeñar las labores de cada uno de los empleados de la empresa.

El bloqueo de navegación se realiza por categorías de acceso; por ejemplo, las páginas de Facebook, Twitter e Instagram, se localizan dentro de la categoría “redes sociales” que está bloqueada en HECC COURRIER.

Siempre que un empelado determine que necesita acceder a una página o a una categoría completa, deberá generar una “Solicitud de cambios y/o servicios”, y solicitar aprobación a su jefe inmediato y al área de sistemas, en dicha solicitud deberá especificar claramente la necesidad de negocio que motiva la solicitud.

El control de las aplicaciones se realiza mediante un estricto control de monitoreo por medio del firewall (Fortinet 60C) se han bloqueado principalmente, las páginas que generan un mayor consumo de ancho de banda, también se bloquean las páginas generadoras de filtraciones de códigos maliciosos y las que podrían perjudicar el correcto funcionamiento de los equipos y dispositivos que se encuentran en la red interna de HECC COURRIER.

3. Identificación de los equipos en las redes

Para la identificación de los equipos en la red LAN de HECC COURRIER, se lleva un estándar en el cual cada equipo tiene un nombre específico para su identificación, el estándar de la identificación de los equipos comienza con la letra inicial del primer nombre, seguido del apellido del empleado, luego un guion al medio y por último las letras “PC” todos estos caracteres deben ser escritos en letras mayúsculas. Por ejemplo, para un empleado de nombre Armando Cabarcas, el nombre de su equipo seria: ACABARCAS-PC

Para identificar equipos conectados a la red LAN, que no son propiedad de HECC COURRIER y que pueden ser posibles ataques a la integridad de la plataforma de red y demás servicios y aplicaciones, se cuenta con

un software llamado “ipscan23.exe” el cual hace escaneo de equipos conectados a cualquier segmento de red de la compañía.
Este es un software gratuito el cual no hay necesidad de instalar, simplemente ejecutándolo funciona correctamente.

RESPONSABILIDADES

El responsable de la seguridad de la información es el encargado de definir procesos para el control actualización y modificación de las redes.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de Control y Gestión de los Servicios de Red	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política de Control y Gestión de los Servicios de Red	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Control y Gestión de los Servicios de Red	Mayo de 2018	

Tabla 28. Formato de Aprobación Politica de Control y Gestión de los Servicios de Red
Fuente: http://www.informationshield.com

1.2.12 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Políticas de Seguridad de la Información					
Política de Transferencia de Información					
Política	IS-12	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 29. Formato de Cabecera Política de Transferencia de Información
Fuente: http://www.informationshield.com

PROPÓSITO:

Definir las directrices de transferencia de información, mitigando el riesgo de fuga o pérdida de información restringida preservando las características de disponibilidad, integridad y confidencialidad.

ALCANCE:

Esta política está dispuesta para todos los funcionarios o empleados de Hecc Courrier.

DETALLE:

La transferencia de información de la organización, entre organizaciones o terceras partes debe estar protegida, controlada y se deben cumplir todas las legislaciones y normas que correspondan.

La organización generará acuerdos de transferencia de información, previa solicitud a la dirección de operaciones. La transferencia de información deberá determinarse a través de un convenio interadministrativo o contrato, el acuerdo de transferencia debe realizarse siguiendo lo establecido. En el tal caso de que sea necesario transferir información confidencial o privada, se deben adoptar controles de cifrado de información de acuerdo con lo establecido en la política de uso de controles criptográficos.

Las características de los acuerdos de transferencia de información en el sftp de Hecc Courrier.

- ✓ Los acuerdos de transferencia de información con organizaciones deberán contener clausulas donde se establezcan las herramientas a utilizar para asegurar la transferencia de información.
- ✓ Establecer los modos que se utilizaran para evitar la interceptación, copiado, modificación y/o destrucción de información.
- ✓ La transferencia de información digital será liderada por el Área de Sistemas, con la coordinación del Área de operaciones en el cual se encuentra la necesidad.
- ✓ La información deberá disponerse en el sftp que es una de las herramientas seguras para la transferencia de información.

Para transferencia de información interna la organización dispondrá del uso de correo electrónico y de una ruta compartida llamada “Transfer” en la cual por área los empleados de cada área respectiva tengan acceso a la carpeta de su área, tener en cuenta que la carpeta compartida del “Transfer” es de uso temporal ya que al final de cada semana el área de sistemas realizara una limpieza de la información dispuesta en la carpeta.

Los empleados de Hecc Courrier no deben mantener conversaciones confidenciales en lugares públicos y oficinas abiertas. Está prohibido descargar cualquier tipo información a través del canal de Hecc Courrier. Es preciso, por lo tanto, no utilizar esta herramienta para ver, escuchar o descargar música, videos o cualquier elemento que provoque la lentitud en el funcionamiento de la red de la organización obstruyendo la labor de los compañeros. No se debe enviar información confidencial a través de correo electrónico. Si se requiere por razones justificadas, debe ser aprobado por la Dirección del área o en su ausencia por una jefatura.

La transmisión de la información se creará teniendo en cuenta la normatividad colombiana vigente, especialmente la relativa a la Ley de Habeas Data (Ley 1266 de 2008), la Ley de Protección de Datos Personales (Ley 1581 de 2012) y Ley de Transparencia y Acceso a la información pública (Ley 1712 de 2014).

RESPONSABILIDADES

Todos los empleados que tengan acceso a la información de la Entidad, deben protegerla de divulgación no autorizada conforme a los Procedimientos de Clasificación y Etiquetado de la Información definidos en el Sistema de Gestión de Calidad. La información sólo podrá ser usada para las actividades autorizadas dentro de los acuerdos suscritos entre Hecc Courrier y las partes interesadas.

En los acuerdos que se establezcan para la transferencia de información, se deben describir: las responsabilidades y procedimientos para la transferencia segura de la información. Para la transferencia de información se deben mitigar los riesgos asociados la pérdida de confidencialidad, integridad o disponibilidad.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de Transferencia de Información	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política de Transferencia de Información	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de Transferencia de Información	Mayo de 2018	

Tabla 30. Formato de Aprobación Política de Transferencia de Información
Fuente: http://www.informationshield.com

1.2.13 POLÍTICA DE RELACIÓN CON LOS PROVEEDORES

Políticas de Seguridad de la Información					
Política de relación con los Proveedores					
Política	IS-15	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 31. Formato de Cabecera Política de relación con los Proveedores
Fuente: http://www.informationshield.com

PROPÓSITO

Definir lineamientos para la gestión de seguridad de la información que debe cumplir los proveedores de servicios, infraestructura o desarrollo para acceder a cualquier tipo de información que sea de la empresa HECC COURRIER.

ALCANCE

Lograr que los proveedores de la empresa HECC COURRIER dentro del marco de seguridad de la información cumplan con lo establecido y acepten los términos y condiciones de su labor.

DETALLE

- ✓ Como principal lineamiento, los proveedores deben tener establecido dentro de su organización un esquema apropiado de seguridad de la Información con normas, estándares y políticas, los cuales serán el soporte a que sus servicios y productos estén asegurados y cumplan debidamente su funcionamiento acorde tanto a la ley como a su reglamento interno.
- ✓ Los proveedores deben tener un esquema de gestión de la seguridad de la información y de control de incidentes capaces de actuar de forma rápida y efectiva en cualquier momento para solucionar inconvenientes con los productos y servicios que adquiere HECC COURRIER.
- ✓ Los proveedores deben tener asegurados los activos de información que van a prestar para HECC COURRIER, ya que intentos de ataque (amenazas) pueden afectar no solo dichos activos de los proveedores sino de HECC COURRIER como tal y de su funcionamiento, ya que la información que se maneja es sensible.
- ✓ Se deben crear acuerdos de confidencialidad entre las partes para asegurar que la información que se maneja dentro de HECC COURRIER no pueda ser divulgada no manipulada por los proveedores sin permiso, ya que de hacerlo se debe establecer sanciones e infracciones acordes a la ley para el tratamiento de información y divulgación.
- ✓ Los proveedores deben asegurar el funcionamiento de sus servicios y productos en un periodo 24/7, ya que de no hacerlo debe acarrear en sanciones con multas económicas que HECC COURRIER debe demandar por incumplimientos.
- ✓ Los proveedores deben demostrar mediante documentos y pruebas el funcionamiento correcto de sus productos y servicios, para así validar que se va a cumplir a cabalidad con lo que HECC COURRIER adquiere con ellos. Ya que sus activos de información no deben ser afectados por alguna falla que se presente en los procesos de la organización si es por un manejo o servicio externo a la compañía.
- ✓ Los proveedores deben aceptar las políticas de gestión de incidentes dentro de HECC COURRIER para asegurar que el funcionamiento de los productos y servicios que brindan en caso de algún inconveniente estén aptos en la resolución y brinden soporte para las soluciones dentro de la empresa.
- ✓ Los proveedores deben cumplir con las regulaciones a nivel local e internacional sobre el tratamiento de la información, así como de su privacidad y seguridad.
- ✓ Los proveedores deben asegurar funcionamiento correcto de sus servicios y productos al momento de efectuar la instalación dentro del área de HECC COURRIER, así mismo el área de Sistemas y operativo debe estar al tanto y verificar dichos procesos para su aprobación.

RESPONSABILIDADES

- ✓ El área de sistemas de HECC COURRIER debe verificar el funcionamiento adecuado de los servicios y productos que los proveedores ofrecen y los cuales han sido instalados en su totalidad. Si

esto no se presenta deben informar de lo sucedido a ambas partes para que se realice pertinentemente o sino determinar las acciones legales por incumplimiento.

- ✓ El área operativa, de sistemas y la gerencia deben realizar documentos legales y acuerdos que determinen la relación con los proveedores, las funciones que debe desarrollar, los servicios que va a brindar y por supuesto las clausulas en caso de incumplimiento tanto de la empresa como de los proveedores.
- ✓ El área de sistemas y operativo debe permitir el acceso a proveedores para procesos de rutina en cuanto a actualización de software, hardware y monitoreo de procesos con los que cuenta la empresa con los servicios y productos que brinda. Debe brindar un acceso limitado a áreas y funciones en los diferentes sistemas a los cuales necesita efectuar mantenimiento o procedimientos.
- ✓ El área operativa y de sistemas debe efectuar revisiones periódicas de la funcionalidad de los productos y servicios que el proveedor está brindando. Así se verificará constantemente que los proveedores estén cumpliendo con su labor y que sus productos estén funcionando debidamente. Cualquier novedad debe estar documentada para llevar un registro de incidentes o eventos en caso de existir.
- ✓ Cada mantenimiento o actualización que los proveedores necesiten hacer de sus productos y servicios deben estar documentadas para que el área de sistemas y operativa puedan validar el funcionamiento de los productos como controles de cambios realizados.
- ✓ La gerencia en su parte legal debe documentar en los acuerdos que deben firmar ambas partes las clausulas a cumplir para que en caso de incumplir algún lineamiento se pueda acceder a entidades legales para que hagan ejercer la ley y efectuar multas por ello.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política de relación con los Proveedores	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política de relación con los Proveedores	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política de relación con los Proveedores Información	Mayo de 2018	

Tabla 32. Formato de Aprobación Política de relación con los Proveedores
Fuente: http://www.informationshield.com

1.2.14 POLÍTICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Políticas de Seguridad de la Información					
Política para la Gestión de Incidentes de Seguridad de la Información					
Política	IS-13	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 33. Formato de Cabecera Política para la Gestión de Incidentes de Seguridad de la Información
Fuente: http://www.informationshield.com

PROPÓSITO

Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata.

ALCANCE

Esta política la deben cumplir todos los empleados de HECC COURRIER.

DETALLE

Todos los funcionarios deben ser conscientes de su responsabilidad para reportar los eventos (o secuencia de eventos) que pueden causar suspensiones en los pasos a seguir del negocio de HECC COURRIER, por ejemplo, fallas de los ordenadores, errores humanos, robo, desastres naturales, etc. De igual manera, se debe reportar las debilidades o vulnerabilidades observadas o sospechadas de los sistemas, aplicaciones, activos o servicios, tan pronto sea posible para evitar que se materialice este riesgo y se generen incidentes de seguridad de la información.

Ningún empleado debe intentar probar las debilidades que detecte o sospeche; en lugar de ello, deberá reportar inmediatamente su hallazgo, el ensayo o prueba de estas debilidades por parte de personas no autorizadas, se interpreta como un uso inadecuado del sistema y en caso de generar daño; HECC COURRIER siguiendo los lineamientos establecidos podrá determinar si el empleado o usuario que lo realizó, tiene una responsabilidad legal o se debe imponer otro tipo de sanción.

Cuando se reporte un incidente de seguridad de la información conforme a la definición de un procedimiento para el reporte de eventos e incidentes de seguridad de la información, se deberá generar el proceso de respaldo y custodia de los activos y los registros del sistema se servidores y equipos. El área de Sistemas, participará activamente en la solución de incidentes que incluyan fallas en el sistema de información, pérdida del servicio, códigos maliciosos, negación del servicio, errores producidos por datos del negocio inconcluso, violaciones de la confidencialidad y la integridad o uso inadecuado de los sistemas de información.

RESPONSABILIDADES

- ✓ El responsable de la seguridad debe poner un protocolo el cual deben entender todos los funcionarios para que sea de su conocimiento cual es el proceso a seguir en caso de presentarse alguna falla. Es decir, cómo y a quien reportarlo para que se tomen los procesos disciplinarios necesarios.

- ✓ El Área de Sistemas debe concientizar y capacitar a los empleados para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política para la Gestión de Incidentes de Seguridad de la Información	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel Leguizamón	Política para la Gestión de Incidentes de Seguridad de la Información	Abril de 2018	
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política para la Gestión de Incidentes de Seguridad de la Información	Mayo de 2018	

Tabla 34. Formato de Aprobación Política para la Gestión de Incidentes de Seguridad de la Información
Fuente: http://www.informationshield.com

1.2.15 POLÍTICA GENERAL DE PROTECCIÓN DE DATOS HECC COURRIER

Políticas de Seguridad de la Información					
Política General de Protección de Datos HECC COURRIER					
Política	IS-07	Fecha efectiva		Email	
Versión	1.0	Contacto		Teléfono	

Tabla 35. Formato de Cabecera Política General de Protección de Datos HECC COURRIER
Fuente: http://www.informationshield.com

PROPÓSITO:

Instaurar las medidas generales para garantizar los niveles de seguridad y privacidad adecuados para la protección de datos personales, con el propósito de evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados

ALCANCE:

HECC COURRIER es consciente de la importancia del correcto tratamiento de los datos personales y por ende está comprometida con el cumplimiento de lo establecido en la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas que las modifiquen, adicionen o complementen. Esta política de protección de datos personales aplica a las bases de datos y archivos que contengan datos personales que sean objeto de tratamiento por parte de HECC COURRIER.

DETALLE:

1) Datos de Clientes

HECC COURRIER establece y cumple cláusulas de confidencialidad dentro de los contratos con los clientes brindándoles confianza acerca del tratamiento de sus datos. Asimismo, cada empleado de HECC COURRIER acepta un acuerdo de confidencialidad que no expira (es decir aplican incluso cuando el empleado se retira) y un código de ética donde se compromete con la seguridad de la información de las partes interesadas de HECC COURRIER**.**

a) Datos Personales Empleados de Clientes HECC COURRIER

Modalidad del Área de Operaciones

HECC COURRIER es el encargado del tratamiento de los datos de empleados de sus clientes en las modalidades de negocio de correspondencia personalizada cumpliendo las actividades normativas que en el marco legal correspondan al encargado de tratamiento de datos, siendo responsable de salvaguardar las bases de datos de los clientes en estas modalidades de negocio, otorgando confidencialidad, integridad y disponibilidad de la información y evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Es responsabilidad del cliente:

- ✓ Obtener la autorización de sus empleados e informarles sobre el uso que tendrán los datos recopilados.
- ✓ Cumplir las actividades enmarcadas en la normatividad vigente, donde se reconocen los deberes y derechos de los titulares de información.
- ✓ Suministrar a HECC COURRIER la información de sus empleados únicamente por los canales de comunicación seguros, certificando que los datos en el sistema son los necesarios para la prestación del servicio de nómina a través de la web y se encuentran únicamente en las bases de datos.

b) Datos Personales Clientes Y Prospectos HECC COURRIER

HECC COURRIER es el responsable del tratamiento de los datos de sus clientes y prospectos. La información se utiliza para fines comerciales:

- ✓ Dar cumplimiento a las obligaciones y acuerdos.
- ✓ Generar negociaciones.
- ✓ Ejecutar actividades de fidelización.
- ✓ Ofrecer e informar sobre nuestros productos y servicios

HECC COURRIER obtiene aprobación del uso de la información de parte de los prospectos a través del formato de Autorización tratamiento de datos prospectos clientes.

2) Datos Personales Empleados HECC COURRIER

HECC COURRIER es el responsable del tratamiento de datos sensibles de sus empleados, los cuales se refieren a aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación. Las directrices del tratamiento de datos están acordadas contractualmente.

3) Datos Personales Proveedores HECC COURRIER

HECC COURRIER es el responsable del tratamiento de datos de sus proveedores con el propósito de:

- ✓ Fortalecer las relaciones comerciales y cumplir las obligaciones contractuales.
- ✓ Dar cumplimiento a las etapas de evaluación, selección, entrega de requisitos, seguimiento y reevaluación de proveedores.
- ✓ Establecer y notificar las responsabilidades a los acuerdos de confidencialidad.
- ✓ Procesar pagos**.**

4) Datos Personales Visitantes de HECC COURRIER

HECC COURRIER es el responsable del tratamiento de datos de sus visitantes. La información se usa exclusivamente para controlar el acceso a las instalaciones de HECC COURRIER, establecer medidas de seguridad y generar datos estadísticos. Esta información debe ser eliminada trascurridos 6 meses de la visita.

5) Generalidades Manejo de La Información

- **Derechos de los Titulares**

  Los titulares de los datos personales que sean tratados por parte de HECC COURRIER tienen los siguientes derechos:

  - ✓ Conocer, actualizar y rectificar sus datos personales que reposan en nuestros registros
  - ✓ Solicitar prueba de la autorización.
  - ✓ Ser informado, previa solicitud, respecto del uso que le han dado a sus datos personales.
  - ✓ Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley de Protección de Datos

Personales, sus decretos reglamentarios y las demás disposiciones que la desarrollen

- ✓ Revocar la autorización y solicitar supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento se ha incurrido en conductas contrarias a las establecidas en la Ley de Protección de Datos Personales, sus decretos reglamentarios y las demás disposiciones que la desarrollen.
- ✓ Acceder de manera gratuita a sus datos personales que hayan sido objeto de tratamiento.

- **Suministro de la Información**

  La información que reúna las condiciones establecidas en la ley podrá suministrarse a las siguientes personas:

  - ✓ Los titulares, sus causahabientes (cuando aquellos falten) o sus representantes legales
  - ✓ Las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
  - ✓ Los terceros autorizados por el titular o por la ley.

RESPONSABILIDADES

- Los empleados que tengan acceso a datos personales tratados y administrados por HECC COURRIER, deberán cumplir con la política aquí descrita, haciendo uso de los controles y medidas establecidas para la protección de la información conforme a su nivel de clasificación.

- El Responsable de las bases de datos que contengan información personal, deberá asegurar que antes de realizar cualquier tratamiento de los datos, HECC COURRIER cuente con las autorizaciones de los Titulares y los mecanismos de control para la protección de la información.

- Los empleados deberán evitar el acceso a los datos personales para los cuales no se encuentren autorizados y en caso de que observen violación o fallas de los mecanismos de control de seguridad y privacidad, deberán ser reportados oportunamente al área de Sistemas para determinar las acciones a desarrollar.

APROBACIÓN

Elaborado	Título	Fecha	Firma
Autores del documento	Política General de Protección de Datos HECC COURRIER	Marzo de 2018	
Revisado	**Título**	**Fecha**	**Firma**
Asesor Ing. Miguel Ángel	Política General de	Abril de 2018	

Leguizamón	Protección de Datos HECC COURRIER		
Aprobado por	**Título**	**Fecha**	**Firma**
La alta gerencia de HECC COURRIER y el Área de Sistemas	Política General de Protección de Datos HECC COURRIER	Mayo de 2018	

Tabla 36. Formato de Aprobación Política General de Protección de Datos HECC COURRIER
Fuente: http://www.informationshield.com