ANEXO B

GUÍA DE IMPLEMENTACIÓN

Tabla de contenido

1. GUÍA DE IMPLEMENTACIÓN 5
1.1 FORMATO DE INVENTARIO DE ACTIVOS 6
1.2 INSTRUCTIVO PARA EL ACCESO A LAS INSTALACIONES DE HECC COURRIER 7
1.3 METODOLOGÍA PARA EL MANEJO DE INFORMACIÓN 9
1.4 INSTRUCTIVO DE REGISTROS AUTOMÁTICOS 11
1.5 INSTRUCTIVO PARA LA SINCRONIZACIÓN DE RELOJES 13
1.6 INVENTARIO DE SOFTWARE LIBRE Y SOFTWARE BASE 13
1.7 INSTRUCTIVO PARA EL MONITOREO DE REGISTROS TÉCNICOS 15
1.8 INSTRUCTIVO DE MANTENIMIENTO DE EQUIPOS 19
1.9 INSTRUCTIVO PARA EL TRASLADO Y RETIRO DE ACTIVOS 20
1.10 PLAN DE EMERGENCIAS 22
1.11 SOLICITUD DE CAMBIOS Y O SERVICIOS 27
1.12 CÓDIGO DE ÉTICA Y CONDUCTA 28
1.13 RECOMENDACIONES GENERALES 31

Lista de Ilustraciones

Ilustración 1. Valoración del Riesgo vs Riesgo..... 5
Ilustración 2. Valoración del Riesgo vs Tiempo..... 6
Ilustración 3. Ciclo de la Información..... 10
Ilustración 4. Herramienta de Monitoreo PRTG..... 16
Ilustración 5. Panel Principal PRTG 17
Ilustración 6. Panel Monitoreo RAM - Herramienta PRTG 17
Ilustración 7. Panel Monitoreo CPU - Herramienta PRTG..... 18
Ilustración 8. Informe Herramienta PRTG 18
Ilustración 9. Esquema Roles Retiro de Activos..... 21

Lista de tablas

Tabla 1. Listado de Software Libre 14
Tabla 2. Listado de Software Base 15
Tabla 3. Aprobación tiempos autorizados 21
Tabla 4. Objetivos de Retiro 22
Tabla 5. Definiciones Emergencias. 24
Tabla 6. Clasificación Emergencias. 24
Tabla 7. Clasificación de las emergencias según la gravedad. 25
Tabla 8. Soportes de Emergencias. 25
Tabla 9. Sectores Funcionales de Emergencias. 26
Tabla 10. Formato de Solicitud de Cambios o servicios. 28

1. GUÍA DE IMPLEMENTACIÓN

De acuerdo a las políticas de seguridad de la información y a la gestión de los riesgos detallados anteriormente, se ha determinado realizar una guía de implementación como sugerencia para implementar el presente sistema de gestión de seguridad de la información descrito. Los autores han efectuado un análisis que permite describir los pasos que la empresa HECC COURRIER debería efectuar para que este diseño SGSI sea efectivo.

Teniendo en cuenta la gestión de los riesgos y la valoración de cada uno de ellos se ha realizado una gráfica que determina cuales deberían ser los que necesitan ser tratados prioritariamente. Identificando la escala de valoración se ha determinado que el Riesgo R1 (Riesgos de Fraude o Corrupción.) como de alto impacto y por el cual encabeza la lista. Aunque algunos riesgos sean demasiado importantes hay que tener en cuenta otra variable como lo es el tiempo de ejecución que este conlleve para realizar.

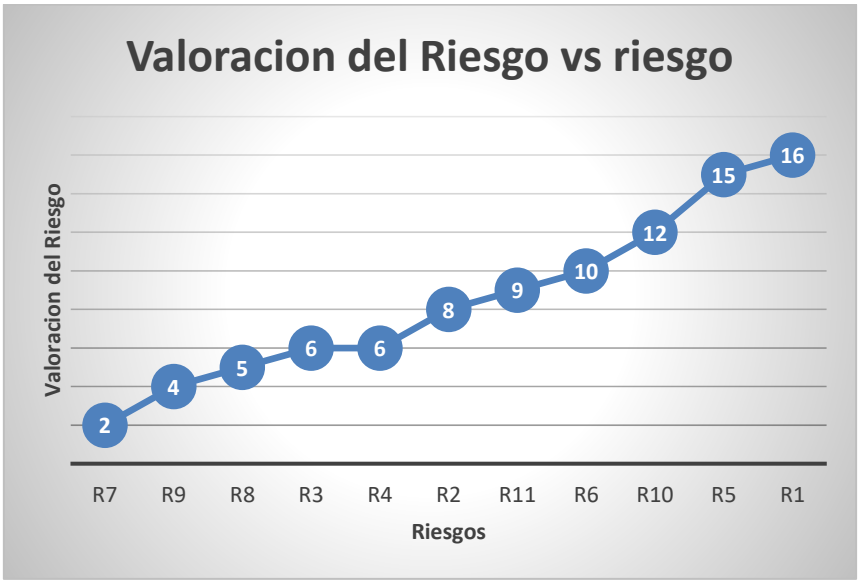


Ilustración 1. Valoración del Riesgo vs Riesgo
Fuente: Los Autores

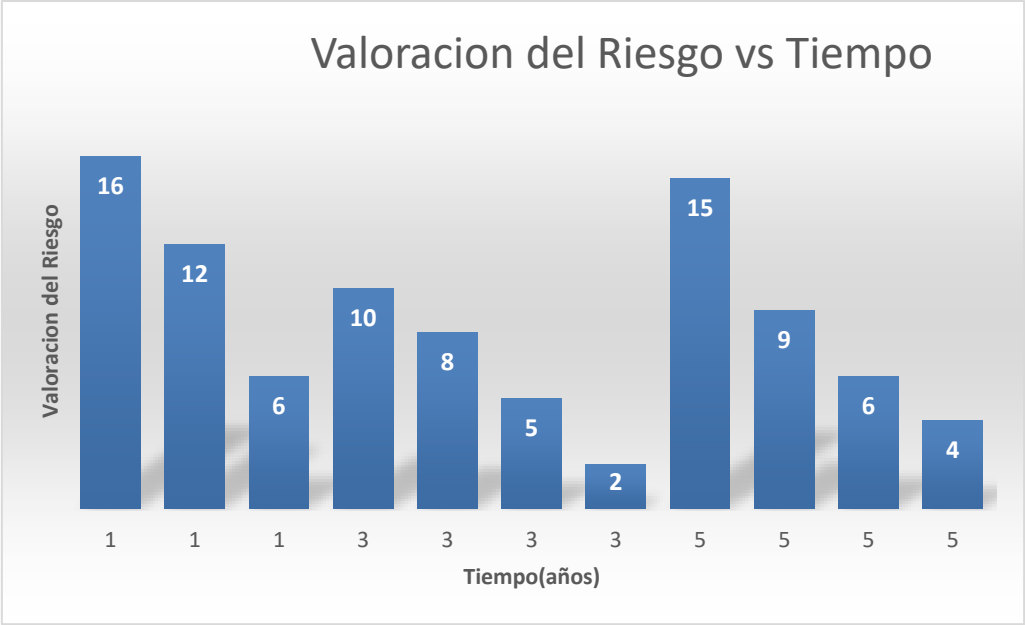


Ilustración 2. Valoración del Riesgo vs Tiempo
Fuente: Los Autores

De acuerdo a las gráficas se creará la guía de implementación abarcando primero la mitigación de los riesgos con valoración más alta pero que llevan menos tiempo de implementación. Se aclara que la guía de implementación es el paso a seguir después establecer y hacer cumplir las políticas antes mencionadas, la guía es complemento y sustento de las políticas desarrolladas. Partiendo del principio que lo primero que se debe hacer es desarrollar las normas y directrices que se mencionan en las políticas.

1.1 FORMATO DE INVENTARIO DE ACTIVOS

Se debe establecer un formato en Excel protegido por contraseña donde se especifique en cada hoja los activos que se encuentran en la organización. Las hojas contendrán las siguientes columnas:

- Hoja de equipo de escritorio
  - ✓ Código de Inventario
  - ✓ Tipo de Activo
  - ✓ Marca
  - ✓ Equipo
  - ✓ Estado
  - ✓ Usuario Actual
  - ✓ Área
  - ✓ Modelo del Equipo
  - ✓ Modelo del Procesador
  - ✓ Velocidad del Procesador
  - ✓ Generación del Procesador(Hz)
  - ✓ Memoria
  - ✓ Disco
  - ✓ Sistema Operativo

- ✓ Precio de Compra
- ✓ Fecha de Compra
- ✓ Fin de Garantía
- ✓ Fecha de Baja
- ✓ Razón de Baja

- Dispositivos de Red
  - ✓ Código de Inventario
  - ✓ Tipo
  - ✓ Marca
  - ✓ Modelo
  - ✓ Serial
  - ✓ Estado
  - ✓ Ubicación
  - ✓ Área
- Impresoras – Scanner
  - ✓ Código de Inventario
  - ✓ Tipo
  - ✓ Marca
  - ✓ Modelo
  - ✓ Serial
  - ✓ Estado
  - ✓ Ubicación
  - ✓ Área
- Servidores
  - ✓ Código de Inventario
  - ✓ Hostname
  - ✓ Tipo
  - ✓ Marca
  - ✓ Modelo
  - ✓ Etiqueta de Servicio
  - ✓ Estado
  - ✓ Ubicación
- Medios Removibles
  - ✓ Código de Inventario
  - ✓ Tipo
  - ✓ Marca
  - ✓ Modelo
  - ✓ Serial
  - ✓ Estado
  - ✓ Ubicación
  - ✓ Área

1.2 INSTRUCTIVO PARA EL ACCESO A LAS INSTALACIONES DE HECC COURRIER

Objetivo:

Controlar el acceso físico a las instalaciones de Hecc Courrier para evitar el daño, interferencia modificación o robo de la información y los activos de la

empresa.

Pautas Generales:

- ✓ En Hecc Courrier se establecen diferentes áreas/departamentos que son controlados por controles físicos de acuerdo a los servicios de procesamiento y al tipo de información que manipula cada uno. Es responsabilidad de todos los empleados dar lectura a este documento y acatar las políticas de acceso aquí descritas.
- ✓ Es responsabilidad del encargado de recepción verificar, administrar y cuidar las tarjetas de acceso de préstamo y de visitantes.
- ✓ Cualquier situación fuera del alcance de este instructivo debe ser tramitada por correo electrónico con el área de Sistemas para definir la gestión adecuada, garantizando el cumplimiento del objetivo que tienen los controles físicos y de acceso.

Controles de Acceso Físico

Los controles de seguridad física con los que cuenta Hecc Courrier son los que se definen en la Política de Seguridad Física y de Entorno (Anexo A Numeral 1.2.7):

1. Sistema de Control de Acceso por Tarjetas de Aproximación
2. Carné de Identificación Para Empleados Y Para Visitantes
3. Control de Visitantes
4. Restricciones de Acceso Según el Tipo de Área

Adicional a lo anterior se cuentan con controles de tipo:

5. Cámaras de Seguridad

   Las cámaras hacen parte de los sistemas de seguridad que velan por el cumplimiento de nuestros acuerdos de confidencialidad internos y con nuestros clientes, por lo tanto, los registros se utilizarán las veces que se estime conveniente ante infracciones al reglamento de trabajo. Las cámaras de seguridad se encuentran distribuidas en las instalaciones de HECC COURRIER especialmente en las áreas de máxima seguridad. Las cuales son administradas y para efectos de revisión de los registros el área de Sistemas tiene usuario de acceso. Cuando un empleado requiere la revisión del registro de vídeo, debe:
   - Enviar por correo electrónico la solicitud al área de gestión humana y área de sistemas, informando la fecha, hora y motivo por el cual se realiza la solicitud.
   - El área de gestión humana verifica si se está presentando una falta al Reglamento interno de trabajo que amerite la revisión del registro, autoriza la solicitud y el área de sistemas procede con la revisión para entregar respuesta al empleado máximo 3 días hábiles después de recibir el correo electrónico.
6. Ingreso de Dispositivos de Propiedad de los Empleados y/o Visitantes a Hecc Courrier

- ✓ Empleados:
  Un empleado puede ingresar un computador personal, siempre y cuando no haga uso del mismo dentro de las instalaciones ni lo conecte a la red de Hecc Courrier a menos que sea autorizado por el área de Sistemas.
- ✓ Visitantes:
  Cuando un visitante requiera ingresar un computador personal lo debe registrar en la recepción. No es permitido conectar los computadores personales a la red de Hecc Courrier sin previa autorización de la dirección del área de sistemas, por lo tanto, el empleado responsable de la visita debe diligenciar con antelación la solicitud de cambios y o servicios, solicitando las autorizaciones y explicando el motivo por el cual se requiere acceso a la red.

1.3 METODOLOGÍA PARA EL MANEJO DE INFORMACIÓN

Objetivo:

Establecer reglas para que la información y documentos no se accedan, divulguen, modifiquen, remuevan o destruyan sin autorización. Definir el manejo que se le debe dar a los registros e información de Hecc Courrier en cuanto a distribución, acceso, recuperación, uso, almacenamiento, conservación y disposición.

Pautas Generales:

- Todo empleado de HECC COURRIER debe cumplir el Acuerdo de confidencialidad.
- Todo empleado debe conocer y cumplir los acuerdos de confidencialidad establecidos contractualmente con los clientes.
- Los derechos patrimoniales de autor sobre las obras creadas por el empleado en ejercicio de sus funciones o con ocasión de ellas pertenecen a HECC COURRIER, por ende, es deber de cada empleado cumplir con la normatividad de propiedad intelectual.
- Es obligación de cada empleado archivar en el lugar correspondiente para evitar pérdidas o demoras al buscar un registro.

Clasificación de La Información

En la Política de Gestión de Activos (Anexo A. Numeral 1.2.3) se establece la clasificación de la información.

Disponibilidad de documentos

1. Distribución y acceso a la documentación

   Para que el personal de Hecc Courrier pueda consultar y usar la documentación de los Sistemas de Gestión de Hecc Courrier, se debe

disponer de una ruta compartida del servidor que sea accesible. Es responsabilidad de los empleados utilizar la documentación vigente de los sistemas de gestión de Hecc Courrier y no guardar documentos en los equipos, lo cual se garantiza consultando los medios ya mencionados.

2. Recuperación

   Es responsabilidad de los empleados guardar la información en los lugares autorizados para garantizar su disponibilidad, integridad y recuperación. Así mismo, en la documentación específica de cada proceso, se establece reglas y directrices para guardar la información. La información física, se debe escanear y guardar en medio electrónico para facilitar su recuperación.

Ciclo de la Información



Ilustración 3. Ciclo de la Información
Fuente: Los Autores

1. Uso

   - ✓ Todos los registros deben ser legibles e identificables.
   - ✓ En los registros impresos en lo posible no se debe usar corrector ni hacer enmendaduras al registro.
   - ✓ Los formatos deben diligenciarse completamente. Es decir, si hay campos que no aplican se debe poner una raya, NA o no aplica

2. Etiquetado

   Se debe definir la clasificación de los documentos según tipo de información.
   Si un trabajador de Hecc Courrier evidencia un documento sin etiqueta y considera que contiene información diferente a la pública, debe reportarlo a al área de sistemas.

3. Transferencia e Intercambio

Los servicios de intercambio de información deben cumplir con la normatividad legal vigente. Se debe cumplir con la Política de Transferencia de Información (Anexo A Numeral 1.2.12). Para el área de Operaciones se encuentra prohibido el intercambio de información producido por canales diferentes a los establecidos. Por ejemplo, video, servicios de pantalla compartida, unidades de almacenamiento en la nube, acceso remoto, etc. En caso de necesitarse se debe contar con aprobación del área de sistemas y de la alta gerencia.

4. Almacenamiento y Preservación

- ✓ En documentos específicos de cada proceso (procedimientos, instructivos, metodologías) se precisa también el lugar de archivo de ciertos registros.
- ✓ Cuando se cambie el lugar u otras características de archivo de un registro se debe actualizar el sistema documental, incluido el listado de registros. El cambio debe ser controlado y notificado por el área de Recursos Humanos mediante correo electrónico.
- ✓ La mayoría de registros se almacena de carpetas compartidas, sin embargo, si se guarda información en cada equipo asignado, esta debe estar en D/Hecc.
- ✓ La información confidencial o privada no se debe guardar en dispositivos externos

1.4 INSTRUCTIVO DE REGISTROS AUTOMÁTICOS

Hecc Courrier para el manejo de registros automáticos debe determinar unas medidas tanto con su la organización interna como la organización externa, en este caso proveedores. Los proveedores quienes suministran servicios e infraestructura a la organización deben determinar el manejo de registros automáticas en cada uno de los componentes que suministran, así se identificarían los fallos o incidentes que se puedan presentar y establecer monitoreos que permitan detallar los eventos y quien los ejecuto en cada uno de sus sistemas.

Los registros automáticos se deben generar y obtener con base en los activos de la empresa, para ello se tienen en sistemas operativos, dispositivos de seguridad, almacenamiento y aplicaciones, así mismo se debe definir una infraestructura de gestión de registros automáticos para que sea escalable, ya que la cantidad de registros irá creciendo en cada evento, configuración o modificación. Se debe capturar todos los registros de los sistemas críticos e infraestructura y componentes de red que tengan manipulación de información sensible, tal es el caso del manejo de transacciones bancarias en el envío de correspondencia.

Los tipos de registros que deben ser capturados y tratados son:

- Accesos de usuario.
- Acceso privilegiado o administrativo.
- Uso de mecanismos de autenticación e identificación.
- Accesos remotos e inalámbricos Cambios en los sistemas o configuración de aplicaciones.
- Accesos a transacciones bancarias.
- Cambios de privilegios de acceso.
- Uso de utilidades del sistema.
- Activación o desactivación de sistemas de seguridad.
- Accesos a registros de auditoria.[1]

Adicionalmente, se describen los requerimientos mínimos que deben tener los registros de eventos:

- Identificación del usuario
- Tipo de evento
- Fecha y hora
- Resultado de la acción (éxito o fallo)
- Origen del evento
- Identidad del recurso afectado[2]

La alta gerencia de Hecc Courrier y el área de sistemas y operativo deben obligar a los proveedores de servicios e infraestructura se adquiera toda la información de los eventos que sucedan en los procesos de Hecc Courrier, con lo cual se podrá tener un monitoreo de las actividades y hacer evaluaciones periódicas de los registros que se presentaran tanto en sistema como en físico para futuras auditorias tanto internas como externas de la empresa. El área de Sistemas también tendrá que establecer dichas configuraciones dentro de los procesos internos que se manejen en cuanto a configuraciones de red, tratamiento de la información, eventos en procesos administrativos, contables y de sistemas.

Para mejorar la implementación de los registros automáticos y los eventos en que se presentan, los autores recomiendan tener en cuenta la herramienta SIEM (Gestión de Eventos de Información de Seguridad) la cual tiene un enfoque de gestión de la seguridad que busca proporcionar una visión holística de la seguridad de la tecnología de la información (TI) de una organización.

Un sistema SIEM centraliza el almacenamiento y la interpretación de los registros y permite un análisis casi en tiempo real que permite al personal de seguridad tomar medidas defensivas más rápidamente. Un sistema SIEM recopila los datos en un repositorio central para el análisis de tendencias y proporciona informes

---

[1] Avella, Julian. Calderon, Leonardo. Mateus, Cristian. Guía metodológica para la gestión centralizada de registros de seguridad a través de un siem. Universidad Catolica de Colombia. 2015. Recuperado de: http://repository.ucatolica.edu.co/bitstream/10983/2847/1/GU%C3%8DA%20METODOL%C3%93GICA%20PARA%20LA%20GESTI%C3%93N%20CENTRALIZADA%20DE%20REGISTROS%20DE%20SEGURIDAD%20A%20TRAV%C3%89S%20DE%20UN%20SIEM.pdf

[2] Acosta, David. Controles técnicos de PCI DSS parte VI: Registro de eventos (logs). PCI Hispano. 2016. Recuperado de: https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-vi-registro-de-eventos-logs/

automatizados para el cumplimiento y la generación de informes centralizados. Al unir estas dos funciones, los sistemas SIEM proporcionan una identificación, un análisis y una recuperación más rápidos de los eventos de seguridad. Esto también permite a los administradores de cumplimiento confirmar que están cumpliendo con los requisitos de cumplimiento legal de una organización.

Un sistema SIEM recoge registros y otra documentación relacionada con la seguridad, para ser analizados. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación de forma jerárquica para recopilar eventos relacionados con la seguridad de dispositivos de usuario final, servidores, equipos de red e incluso equipos de seguridad especializados como firewalls, antivirus o sistemas de prevención de intrusiones. Los recolectores envían eventos a una consola de administración centralizada, que realiza inspecciones y señala anomalías. Para permitir que el sistema identifique eventos anómalos, es importante que el administrador de SIEM cree primero un perfil del sistema en condiciones normales de evento.[3]

1.5 INSTRUCTIVO PARA LA SINCRONIZACIÓN DE RELOJES

Hecc Courrier tendrá en cuenta el protocolo NTP (Network Time Protocol) - Protocolo de Internet para sincronizar los relojes) este posee o realiza el proceso de sincronizar los relojes de los ordenadores en la red con el directorio activo, este a su vez realiza sincronizado con el instituto nacional de metrología de Colombia (INM) y el cual establece la hora legal para Colombia.

1.6 INVENTARIO DE SOFTWARE LIBRE Y SOFTWARE BASE

HECC COURRIER debe establecer un inventario de software libre y base para el funcionamiento de su plataforma y servicios que proveen, este debe estar descrito de la siguiente forma:

Listado de Software Libre

SOFTWARE	FUNCIONALIDAD	LINK DE SOPORTE FREE
7ZIP	Compresión de archivos	http://www.7-zip.org/
WINSCP	Herramienta de conexión de sftp	https://winscp.net/eng/docs/lang:es
GOOGLE CHROME	Navegador Web	https://support.google.com/chrome/answer/95346?hl=es-419
FIREFOX	Navegador Web	https://www.mozilla.org/es-ES/about/legal/terms/services/
PUTTY	Cliente SSH, Telnet, login, y TCP raw con licencia libre	http://www.putty.org/
STUNNEL	Programa libre multi-plataforma, utilizado para	https://www.stunnel.org/index.html

[3] Rouse, Margareth. Gestión de eventos e información de seguridad (SIEM). Search DataCenter en Español. 2017. Recuperado de: http://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

	la creación de túneles TLS/SSL	
VLC MEDIA PLAYER	Reproductor multimedia	https://www.videolan.org/vlc/index.es.html

Tabla 1. Listado de Software Libre
Fuente: Los Autores

El área de Sistemas debe garantizar que todos los equipos de la organización tengan instalado los siguientes software base; deben estar siempre en su última versión liberada.

- ✓ Office
- ✓ Google Chrome
- ✓ Adobe Reader
- ✓ 7Zip
- ✓ Antivirus Symantec

De acuerdo con las actividades realizadas por los diferentes cargos y departamentos, se debe tener definido en una matriz con el software base requerido para realizar sus actividades.

Gestión de actualización de software base

Con el fin de gestionar y controlar las posibles vulnerabilidades que se pueden presentar por la falta de instalación de las actualizaciones del software base, a continuación, se presenta la matriz de identificación y proceso de instalación correspondiente.

SOFTWARE BASE	IDENTIFICACION DE ACTUALIZACIONES	INSTALACION DE ACTUALIZACIONES	VULNERABILIDADES POR DESACTUALIZACION
OFFICE	Office realiza en los sistemas operativos de Hecc Courrier (Win7, Win8 y Win10) automáticamente las actualizaciones que se encuentren liberadas por el proveedor las cuales resuelven vulnerabilidades de seguridad.	Automáticamente	✓ Vulnerabilidad de no poseer accesos a las plantillas en línea. ✓ Vulnerabilidad de un atacante puede ejecutar código arbitrario. ✓ Vulnerabilidad de corrupción de memoria.
GOOGLE CHROME	Google Chrome realiza automáticamente las actualizaciones que sean liberadas por el proveedor en todos los equipos de Hecc Courrier. .	Automáticamente	✓ Vulnerabilidad de asumir el riesgo de desarrollar o mantener productos para una plataforma sin soporte. ✓ No podrá utilizar ciertos componentes en páginas electrónicas. ✓ Vulnerabilidad contra suplantación de identidad y software malicioso. ✓ Vulnerabilidad de

			instalación de certificados SSL.
ADOBE READER	Adobe Reader genera alertas de actualización la cual se debe ejecutar manualmente por el usuario perfilado administrador.	Manualmente	✓ Vulnerabilidad de no poder utilizar ciertos componentes del aplicativo. ✓ Vulnerabilidad de no poder ejecutar archivos si el aplicativo no está actualizado. ✓ Vulnerabilidad de seguridad y correcciones de errores.
7 ZIP	7Zip genera alertas de actualización la cual se debe ejecutar manualmente por el usuario perfilado administrador.	Manualmente	✓ Vulnerabilidad de ejecución de código arbitrario. ✓ Vulnerabilidad de ejecución de bibliotecas en software de terceros. ✓ Vulnerabilidad en el código que maneja el formato UDF.
ANTIVIRUS SYMANTEC	Symantec envía un reporte de actualización por medio de correo en el cual indica que equipos deben reiniciar para actualizar automáticamente las definiciones de virus. El área de sistemas envía un correo a los usuarios indicados en el informe para que reinicien el área de sistemas realiza el seguimiento si el usuario realiza el reinicio del equipo por medio de la plataforma manager de Symantec en la cual informa si no se ha realizado el procedimiento. Al no reiniciar el área de sistemas realiza el reinicio del equipo remotamente.	Automáticamente	✓ Vulnerabilidad de desactualización de definiciones de virus. ✓ Vulnerabilidad de ejecutar software mal intencionado. ✓ Vulnerabilidad de robo de información. ✓ Vulnerabilidad de suplantación de identidad. ✓ Vulnerabilidad de reenvió de software mal intencionado. ✓ Vulnerabilidad de daño de hardware. ✓ Vulnerabilidad de envió de spam. ✓ Vulnerabilidad de escaneo en busca de virus. ✓ Vulnerabilidad de instalación de software mal intencionado

Tabla 2. Listado de Software Base
Fuente: Los Autores

1.7 INSTRUCTIVO PARA EL MONITOREO DE REGISTROS TÉCNICOS

Objetivo:

Implementar una herramienta para el monitoreo de la carga de los servidores de producción, la disponibilidad de los servicios, disponibilidad de cada una de las

bases de datos de Hecc Courrier y elaborar informes detallados.

Generalidades:

A Hecc Courrier se le recomienda la herramienta PRTG (Paessler Router Traffic Grapher) para realizar el monitoreo de todos los servicios y servidores. Se pueden parametrizar sensores para el monitoreo de la disponibilidad. De igual manera se monitorea la disponibilidad de los servidores y la carga que presentan los recursos (RAM, CPU, etc.) de cada uno.

Ingreso a la herramienta de monitoreo

La administración de la plataforma de la herramienta se realiza a través de un acceso web



Ilustración 4. Herramienta de Monitoreo PRTG
Fuente: https://pt.slideshare.net/Romario2006/prtg

El panel principal muestra todos los sensores que se tienen parametrizados y el estado de cada uno.

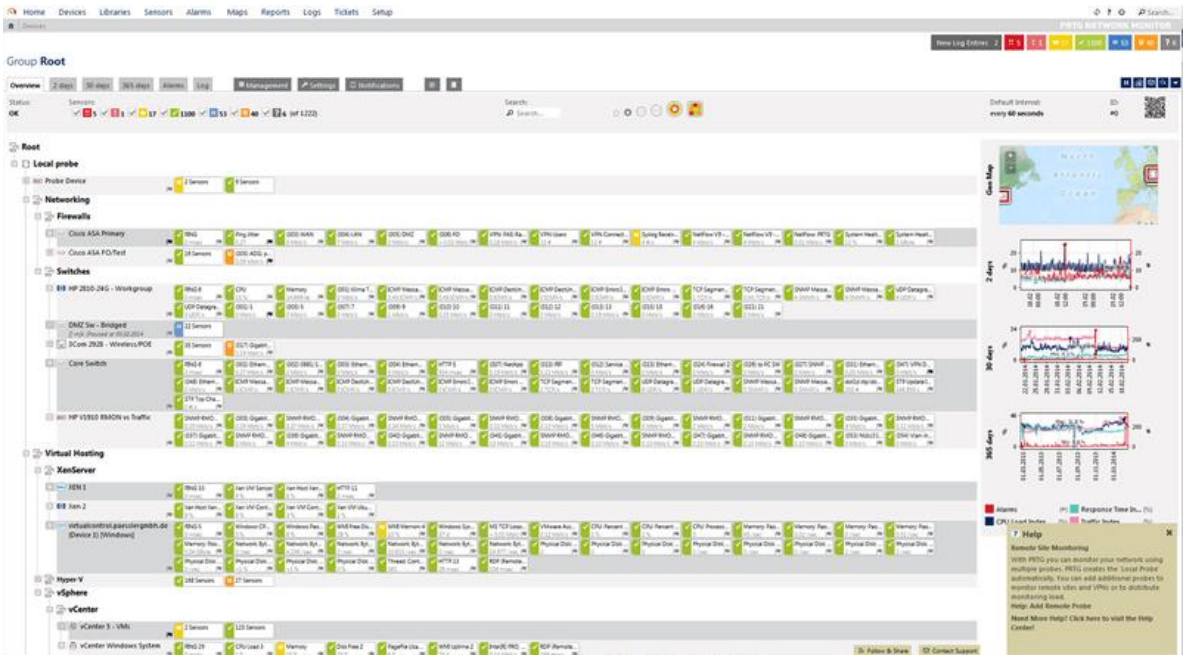


Ilustración 5. Panel Principal PRTG
Fuente: http://telecom-academy.blogspot.com.co/2018/01/PRTG-Network-Monitor-Software-with-sensor-free-download.html

Monitoreo de Recursos de Servidores

Los recursos de los servidores que se monitorean son memoria RAM y CPU, para esto se cuenta con sensores que realizan una validación constante de la carga que tiene cada uno de estos. A continuación, se evidencia un ejemplo de la forma en que PRTG muestra el rendimiento de cada uno de estos recursos.

✓ Ram

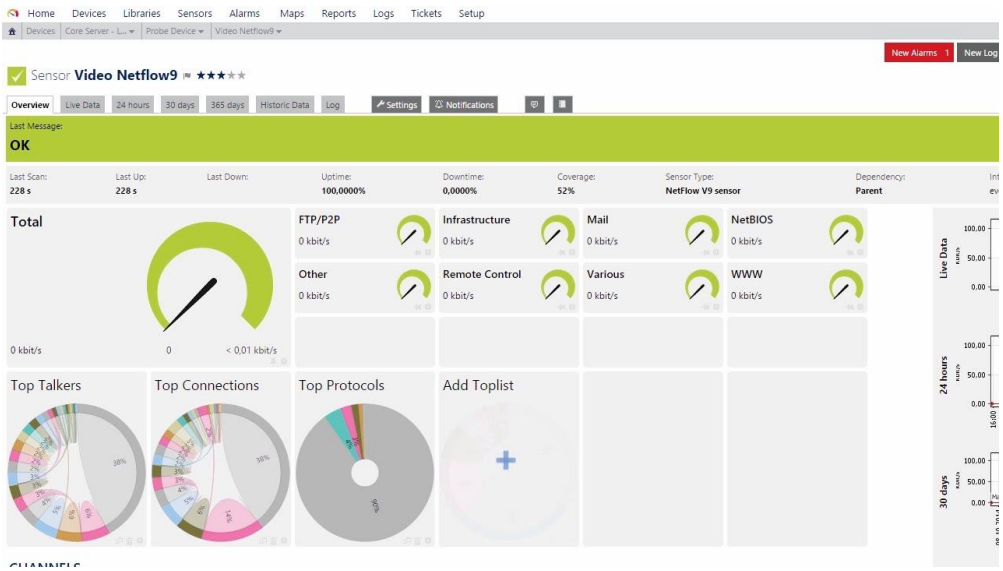


Ilustración 6. Panel Monitoreo RAM - Herramienta PRTG
Fuente: https://www.youtube.com/watch?v=_UrBi859AmI

✓ CPU

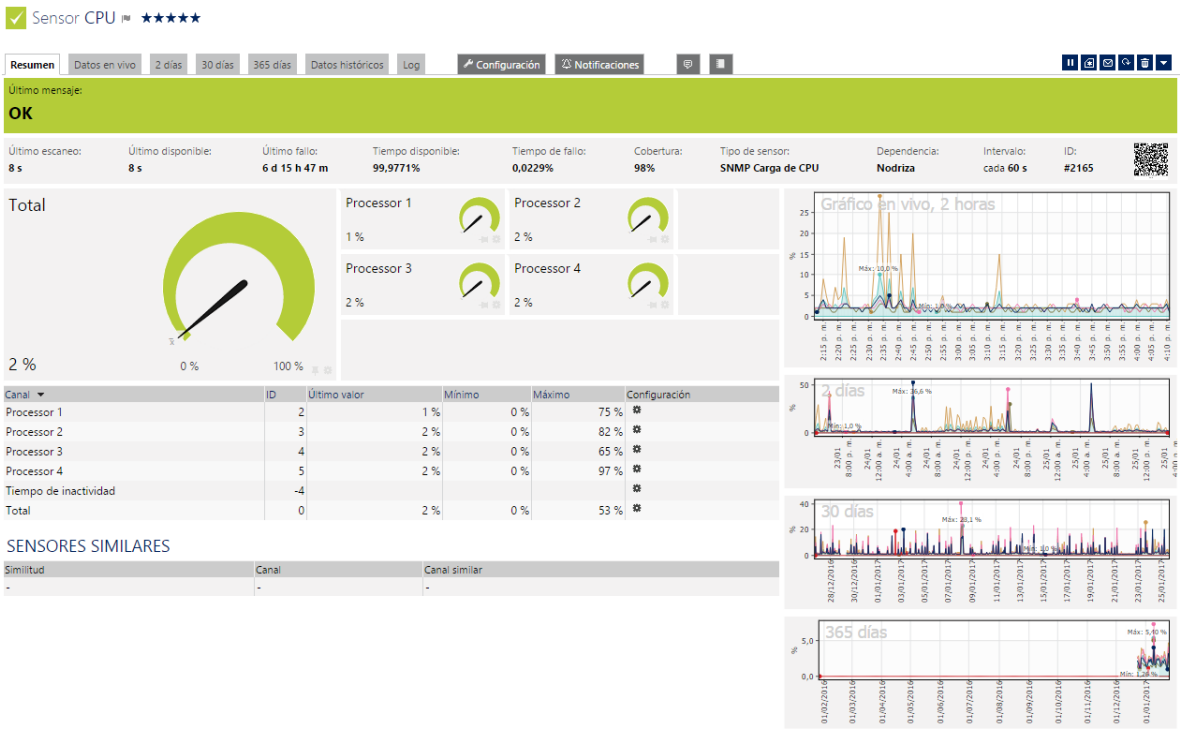


Ilustración 7. Panel Monitoreo CPU - Herramienta PRTG
Fuente: https://www.youtube.com/watch?v=_UrBi859AmI

Los informes que se tienen parame trizados se generan mensualmente y muestran en detalle el comportamiento de cada uno de los recursos de los servidores (Memoria RAM, CPU, etc). Igualmente, el informe muestra la disponibilidad del servidor y de la aplicación. Estos informes son enviados automáticamente al correo del área de sistemas.

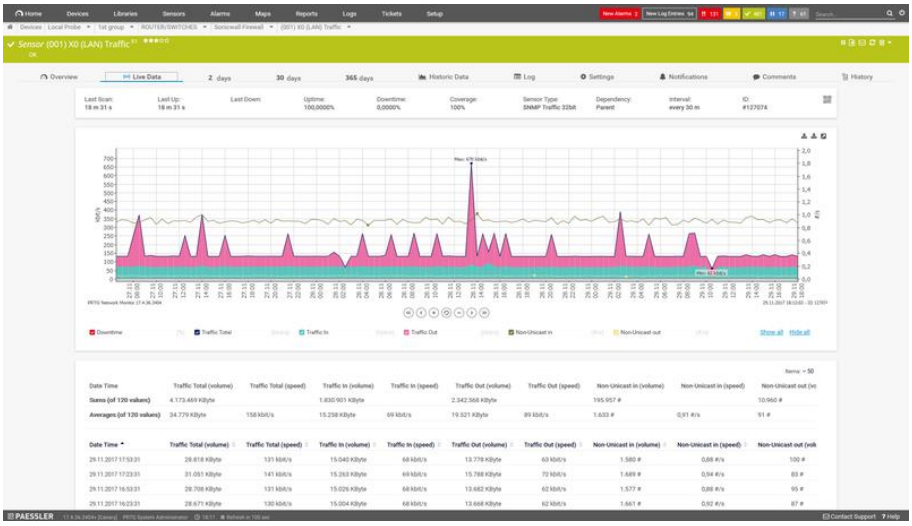


Ilustración 8. Informe Herramienta PRTG
Fuente: https://www.es.paessler.com/prtg

1.8 INSTRUCTIVO DE MANTENIMIENTO DE EQUIPOS

Objetivo

Realizar los mantenimientos preventivos de una forma adecuada para evitar daños físicos y/o lógicos en los equipos de cómputo de la compañía, logrando prevenir las incidencias antes de que estas ocurran. Corregir los daños, problemas y/o fallas que presenten los equipos de cómputo de la compañía.

Mantenimientos para estaciones de trabajo

Para la ejecución del mantenimiento se debe coordinar previamente con el usuario final para validar disponibilidad (día y hora) y además se debe enviar una solicitud de cambios yo servicios indicando la fecha en la cual se ejecutará.

1. Nivel Lógico
   - ❖ Ejecutar un scandisk para verificar y reparar los sectores del disco.
   - ❖ Desfragmentar el disco.
   - ❖ Eliminar archivos temporales, cache de navegadores y Windows.
   - ❖ Optimización de memoria virtual y procesadores.
   - ❖ Optimización de espacio en las particiones.
   - ❖ Instalación de últimas actualizaciones de sistema operativo.

2. Nivel Físico
   - ❖ Limpieza general de hardware.
   - ❖ Realizar diagnóstico de hardware.
   - ❖ Evaluar las características de dispositivos de hardware (memoria y disco) y emitir recomendaciones al respecto.
   - ❖ Evaluar periféricos (mouse, monitor y teclado).

Al finalizar se da respuesta a la solicitud indicando las actividades realizadas y se debe realizar el registro del mantenimiento.

Mantenimientos Correctivos

Los daños que un mantenimiento correctivo (computadores, impresoras, servidores) puede reparar son los siguientes:

- ❖ Corrección de daños tanto en el hardware, como en el software.
- ❖ Reinstalación de los sistemas operativos.
- ❖ Limpieza de software. (virus, troyanos, software espía).
- ❖ Eliminación de los errores de programación de seguridad (Bug).
- ❖ Reparación o sustitución del hardware.
- ❖ Detección de fallos en discos duros, memoria, tarjetas de video, Boards.

Los funcionarios de Hecc Courrier envían la solicitud de cambios y/o servicios indicando las fallas presentadas. Una vez finalizada la reparación por parte del

área de sistemas, se da respuesta a la solicitud indicando actividades realizadas y se debe realizar el registro del mantenimiento.

Mantenimiento y Reinicio de Servidores

Periódicamente se realiza reinicio y/o mantenimiento a los servidores de producción. Estos mantenimientos son programados a inicio de año y lleva un registro trimestral en el formato. Para la ejecución de los mantenimientos se genera solicitud de cambios yo servicios indicando la fecha en la cual se va a realizar.

1. Nivel Lógico
   - ❖ Bajar los servicios desde la consola de administración de servicios en los servidores.
   - ❖ Eliminar archivos temporales, cache de navegadores y Windows.
   - ❖ Instalación de últimas actualizaciones de sistema operativo.
   - ❖ Reiniciar servidor.

1. Nivel Físico
   - ❖ Limpieza general de hardware.
   - ❖ Evaluar las características de dispositivos de hardware (memoria y disco) y emitir recomendaciones al respecto.
   - ❖ Evaluar periféricos (mouse, monitor y teclado).

Finalizada esta actividad se registra.

Aplicación de Actualizaciones de Software

Las actualizaciones del sistema operativo de los servidores se realizan mensualmente. Para realizar estas actualizaciones en los servidores, se debe seguir los siguientes pasos:

- ❖ Iniciar la búsqueda de actualizaciones en “Windows Update”.
- ❖ Ejecutar la instalación de todas las actualizaciones disponibles.
- ❖ Realizar el reinicio del servidor.
- ❖ Una vez reiniciado el servidor, se debe validar que no existan más actualizaciones pendientes, en caso de haberlas se debe ejecutar la instalación y reiniciar nuevamente.
- ❖ Validar la instalación de las actualizaciones en “Actualizaciones instaladas”.
- ❖ Realizar el registro de estas actualizaciones.

La instalación de las actualizaciones de los equipos de escritorio se realiza a través de una política del directorio activo, la cual obliga a cada uno de los equipos a realizar la búsqueda e instalación de las actualizaciones disponibles.

1.9 INSTRUCTIVO PARA EL TRASLADO Y RETIRO DE ACTIVOS

Objetivo

Establecer los parámetros básicos que deben seguir los empleados de Hecc

Courrier para realizar la autorización y retiro de activos de las instalaciones de Hecc Courrier. Ningún activo (hardware, dispositivos de red, bienes muebles o elementos) se deben retirar sin previa autorización y sin asegurarse que cumplen con los controles de seguridad establecidos.

Pautas Generales

Este documento contiene los lineamientos necesarios para el retiro de los activos del interior de Hecc Courrier sin poner en riesgo la confidencialidad e integridad de los activos de la organización. Todo hardware, propiedad de Hecc Courrier se encuentra identificado con el sello de control de activos, si un empleado detecta que el activo no se encuentra identificado, informa al área de sistemas para su pronta identificación.

Personal de aprobación retiro de activos

En Hecc Courrier los únicos empleados que tienen potestad para autorizar el retiro de activos del interior de Hecc Courrier; previa aprobación del jefe inmediato (quien conoce si el empleado tiene una razón de negocio para sacar este activo), son:

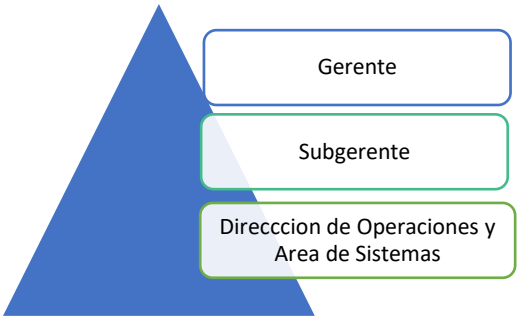


Ilustración 9. Esquema Roles Retiro de Activos
Fuente: Los Autores

La aprobación de la Dirección de Operaciones se tomará como válida solamente cuando no se encuentren ninguno de los anteriores entes de aprobación. Los tiempos de préstamo o mantenimiento se establecen de la siguiente manera:

TIPO	TIEMPO AUTORIZADO
Mantenimiento	Se autoriza que los activos estén fuera de las instalaciones el tiempo que dure el mantenimiento; haciendo seguimiento para que se cumplan los tiempos establecidos
Préstamo	El tiempo de préstamo lo define quien realiza la solicitud de préstamo.

Tabla 3. Aprobación tiempos autorizados
Fuente: Los Autores

Directrices

- Ningún activo (equipo, software, bien mueble o elemento), se debe retirar sin autorización previa.
- Debe existir un responsable de la custodia del activo mientras se encuentre fuera de las instalaciones de Hecc Courrier, el custodio es la

misma persona que solicita sacar el equipo. Esta directriz no aplica para bienes mobiliarios.

- Quien solicita sacar el activo debe asegurar que cumple las disposiciones establecidas para seguridad de equipos fuera de la organización, computación móvil y trabajo remoto. Esta directriz no aplica para bienes mobiliarios.

Procedimiento para el Retiro de Hardware, Dispositivos de Red, Bienes Muebles y Elementos

Independientemente del objetivo con el que pretende retirar los activos del interior de Hecc Courrier el solicitante debe:

a. Identificar el activo a retirar

   Establecer si el activo a retirar es:

   - SOFTWARE: conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas.
   - HARDWARE: conjunto de los componentes que integran la parte material de un equipo utilizado en Hecc Courrier.
   - DISPOSITIVOS DE RED: conjunto de equipos informáticos conectados entre sí que permiten el intercambio de información.
   - BIENES MOBILIARIOS: corresponden a los objetos que sirven para facilitar el desarrollo de las actividades en oficina como mesas, sillas, estanterías etc.

b. Establecer el objetivo del retiro

ACTIVIDAD	DESCRIPCION
Mantenimiento	Toda acción realizada que tienen como objetivo mantener un activo o restaurarlo a un estado en el cual pueda llevar a cabo alguna función requerida
Eliminación	Acción realizada para destruir física y lógicamente algún activo de la organización de Hecc Courrier que no presta su función requerida

Tabla 4. Objetivos de Retiro
Fuente: Los Autores

c. Generar la solicitud.

1.10 PLAN DE EMERGENCIAS

Objetivo

Garantizar la integridad física de los empleados y visitantes de Hecc Courrier y salvaguardar los activos críticos necesarios para la prestación de los servicios ofrecidos por la empresa, minimizando la probabilidad de generación de daños y pérdidas (humanas, materiales, ambientales, etc.), mediante el establecimiento de estrategias y pasos que deben seguir las personas ante la ocurrencia de una

emergencia al interior de Hecc Courrier y el establecimiento de lineamientos administrativos y operativos necesarios para responder satisfactoriamente ante dichos eventos, lo cuales además soportan los requisitos establecidos en la legislación laboral Colombiana, entre ellos principalmente:

- Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), especialmente la Resolución 1016 de 1989. Ley 46 de 1988 “sistema nacional para la prevención y atención de desastres y Decreto 919 de mayo de 1989 Organiza el Sistema Nacional para la Prevención y Atención de Desastres
- Ley 1562 de julio de 2012, por la cual se modifica el sistema de riesgos laborales y se dictan otras disposiciones en materia de salud ocupacional
- Ley 1523 de abril de 2012; por el cual se adopta la política nacional de gestión del riesgo de desastres y se establece el sistema nacional de gestión del riesgo de desastres y se dictan otras disposiciones.

Directrices

Promover el establecimiento, conocimiento y ejecución de estrategias que minimicen el impacto generado por la ocurrencia de las amenazas identificadas en las instalaciones de Hecc Courrier, preservando la vida e integridad de las personas que se encuentren en las instalaciones (colaboradores, proveedores, clientes y visitantes en general), fomentando la cultura de:

- Prevención
- Minimización y
- Control de las emergencias

Proporcionado los recursos humanos, técnicos y financieros que se requieran para la implementación, mantenimiento y mejora del plan de emergencias.

Actualización y divulgación del plan de emergencia

El plan ante emergencias “plan de prevención, preparación y respuesta ante emergencia” debe ser revisado por el Líder Brigadista en conjunto con la Brigada de emergencia o por quien designe la Dirección de Gestión Humana mínimo una vez al año o cuando se presente alguna de las siguientes premisas:

- Al presentarse una situación de emergencia.
- Al identificar nuevas amenazas.
- Por cambios en la estimación de las vulnerabilidades y cálculo del riesgo
- Por cambio de las instalaciones de alguna de sus sedes.

La divulgación del cambio realizado se hace por correo electrónico y el líder brigadista coordina la sensibilización del plan ante emergencias a todos los empleados.

Información general

1. Se debe establecer la población de la organización, cuantos hombres, cuántas mujeres.

2. Establecer la actividad económica de la organización.
3. Tener una descripción clara de la organización
4. Recursos para atención de emergencias:
    - ❖ Humano: Brigada de emergencias conformada por más de 7 empleados de Hecc Courrier.
    - ❖ Físicos - botiquín: Ubicación se encuentra en la dirección de gestión humana.
    - ❖ Físicos – extintores: Ubicación se debe ubicar un extintor por área.
    - ❖ Sistemas de comunicaciones: Telefonía e internet.

5. Marco Conceptual

Definiciones

TERMINO	DEFINICION
Emergencia	Es toda situación que implique un estado de perturbación parcial o total de un sistema, generalmente ocasionado por la probabilidad de ocurrencia o la ocurrencia real de un evento indeseado.
Plan para emergencias	Es un conjunto de procedimientos técnicos y administrativos de prevención y control de riesgos que permite organizar y optimizar los recursos de la empresa, con el fin de evitar o reducir al mínimo las posibles consecuencias humanas y/o económicas que puedan derivarse de una situación de emergencia.
Brigada de emergencia	Es el conjunto de personas especialmente entrenadas, capacitadas y organizadas para la prevención y actuación en accidentes dentro del ámbito laboral.

Tabla 5. Definiciones Emergencias.
Fuente:http://repository.unilibre.edu.co/bitstream/handle/10901/10950/trabajo%20de%20grado.pdf?isAllowed=y&sequence=1

Clasificación de las emergencias

ORIGEN	DESCRIPCION
Natural	Son todas aquellas ocasionadas en forma directa o indirecta por fenómenos naturales como: sismos, inundaciones, huracanes, maremotos, tormentas, vendavales y erupciones volcánicas
Tecnológica	Son aquellas inherentes a los procesos, equipos, materias primas e insumos, desarrollados y utilizados por las empresas, de acuerdo con la actividad económica, entre los cuales se encuentran: Incendios, explosión, derrame de líquidos, colapso estructural o contaminación ambiental.
Social	Son aquellas emergencias producidas por desórdenes de tipo social, como: amenazas, atentados terroristas, robos y secuestros

Tabla 6. Clasificación Emergencias.
Fuente:http://repository.unilibre.edu.co/bitstream/handle/10901/10950/trabajo%20de%20grado.pdf?isAllowed=y&sequence=1

Clasificación de las emergencias según la gravedad

GRAVEDAD	DESCRIPCIÓN
Conato de Emergencia	Emergencia local, que puede controlarse de manera sencilla por el personal del área y afecta un pequeño sector de la empresa. La activación de los recursos necesarios para atenderla depende del Líder Brigadista.
Emergencia	Se presenta en un sector específico de la empresa, pero por sus

Parcial	características requiere otros recursos internos o externos, los cuales se activan en forma automática pero no total. Pero por sus implicaciones no requieren la participación de la alta dirección de la empresa en forma inmediata
Emergencia General	Por sus características, magnitud e implicaciones requiere intervención inmediata, masiva y total de los recursos internos y externos, incluyendo la alta dirección. Para su control requiere la actuación de todos los equipos y brigada.

Tabla 7. Clasificación de las emergencias según la gravedad.
Fuente:http://repository.unilibre.edu.co/bitstream/handle/10901/10950/trabajo%20de%20grado.pdf?isAllowed=y&sequence=1

Vulnerabilidad

Es el grado relativo de sensibilidad para la estabilidad de un sistema, ante las consecuencias de un riesgo, en unas condiciones dadas de seguridad respecto al mismo. Por lo tanto, entre mayor sea la forma como se pueda afectar la estabilidad del sistema, mayor será la vulnerabilidad de dicho sistema ante el riesgo que se considere.

Análisis de vulnerabilidad

Se basa en un inventario de los recursos físicos, técnicos y humanos de la empresa, con objeto de poder determinar los eventuales efectos de distintas modalidades de desastres y señalar la manera como se puede responder ante una amenaza; para facilitar las decisiones estratégicas de los planes operativos, es necesario identificar y evaluar aquellos eventos de mayor probabilidad de ocurrencia.

Organización del plan para emergencias

Soportes

Para que las acciones de prevención y control de las situaciones de emergencia, así como las acciones posteriores a la misma, tendientes a superar dicho estado puedan ejecutarse convenientemente, se requiere de cuatro pilares de soporte al plan de prevención, preparación y respuesta ante emergencias, ellos son:

SOPORTE	DESCRIPCIÓN
Financiero	Que permita recuperar las pérdidas sufridas y la capacidad operacional, mediante un plan de seguros o financiación de los recursos internos, créditos o aportes de otros orígenes.
Tecnológico	Que suministre herramientas operacionales para el control de las emergencias; por ejemplo, sistemas de comunicación.
Operacional	Mediante el diseño, enseñanza y práctica de procedimientos de acción específicos en cada una de las áreas.
Organizacional	Mediante una estructura que permita diseñar y administrar el plan de prevención, preparación y respuesta ante emergencias, definir funciones y responsabilidades y capacitar a cada una de las personas involucradas. Lo anterior incluye el organigrama de emergencia.

Tabla 8. Soportes de Emergencias.
Fuente: http://docplayer.es/3719728-Universidad-francisco-de-paula-santander-ocana-documento-formato-hoja-de-resumen-para-trabajo-de-grado-resumen-trabajo-de-grado.html

El soporte organizacional del plan de prevención, preparación y respuesta ante emergencias de Hecc Courrier, está constituido por sectores funcionales como se describen a continuación:

SECTOR FUNCIONAL	DESCRIPCIÓN
Comité de Emergencias	Máxima instancia operacional durante las fases de prevención, control y mitigación de la emergencia; es el responsable de la implementación del plan y quien se constituye a su vez, en el máximo nivel de decisión operativa en el caso de una emergencia.
Grupo Interno	Conformado por el Líder Brigadista y miembros de la Brigada de Emergencia. Este grupo de trabajo está constituido por empleados voluntarios distribuidos en las diferentes áreas y regionales, quienes han recibido capacitaciones en Primeros Auxilios y Evacuación.
Grupos de Operación Externos	Conformados por las instituciones que pueden operar en caso de emergencia

Tabla 9. Sectores Funcionales de Emergencias.
Fuente: http://docplayer.es/3719728-Universidad-francisco-de-paula-santander-ocana-documento-formato-hoja-de-resumen-para-trabajo-de-grado-resumen-trabajo-de-grado.html

Se deberán establecer:

Procedimientos Operativos Normalizados

Los procedimientos son un mecanismo necesario para realizar las actividades de control determinantes en una situación de emergencia, como:

- Procedimiento en caso de incendio y/o explosión.
- Procedimiento para evacuación.
- Procedimiento en caso de terremoto.
- Procedimiento por emergencias en descargas eléctricas.
- Procedimiento por emergencia médica.
- Instrucciones generales en caso de amenaza terrorista (bomba).
- Procedimiento general en caso de emergencia en horario no laboral.

Plan De Evacuación

El objetivo de un simulacro es verificar en sitio y tiempo real, la capacidad de respuesta de las personas y la organización operativa del plan para emergencias ante un evento de posible ocurrencia, basado en los procedimientos para emergencias.

El Plan De Evacuación Tiene Aplicación En Los Siguientes Eventos

a. En caso de incendio, presencia de humo o atmósferas enrarecidas: siempre se dará la orden de evacuar las instalaciones.
b. En caso de amenaza o sospecha de bomba, se evacuarán todas las dependencias previa evaluación de la situación, por parte del comité de emergencia y el oficial de seguridad de la información
c. En caso de explosión, una vez se ha producido una explosión en cualquiera de las áreas, se deberá adelantar una evacuación total, mientras se hace revisión de toda la edificación, por parte de personal especializado.
d. En caso de terremoto, la evacuación se ordenará una vez cese el movimiento telúrico activando la alarma para evacuación.

1.11 SOLICITUD DE CAMBIOS Y O SERVICIOS

Se recomienda trabajar la siguiente tabla para solicitud de cambios o servicios para el área de sistemas.

SOLICITANTE

TIPO DE SOLICITUD	AREA SOLICITANTE	PRIORIDAD
Cambio:		**Alta (inmediata)**
Servicio:		**Media (normal)**
Falla:		**Baja**

SELECCIONE EL TIPO DE SOLICITUD DE ACUERDO A:
Servicio: Actividades a realizar para que el personal de la compañía pueda llevar a cabo sus labores, que no causan impacto ni necesitan un plan de pruebas. **Cambios**: Son aquellos que involucran un impacto en el desempeño de un aplicativo o plataforma, e incluyen plan de pruebas y plan de ejecución. **Falla:** Eventualidades que afectan el servicio en la compañía.

DESCRIPCIÓN DEL CAMBIO Y/O SERVICIO

IMPACTO Y RIESGOS ASOCIADOS AL CAMBIO(En que beneficia o afecta el cambio propuesto)

PLANES ASOCIADOS AL CAMBIO (Diligenciar en caso de que el tipo de solicitud sea cambio)		
PLAN	**TAREAS**	**RESPONSABLE(S)**
PLAN DE EJECUCIÓN	Pasos…	
PLAN DE REVERSIÓN (Roll-back)	Pasos…	

DATOS DEL SOLICITANTE Y APROBACIONES RESPECTIVAS			
	Nombre	**Cargo**	**Fecha**
Solicitante:			
Aprobación 1			
Aprobación 2			
Aprobación 3			

Nota 1: Todas las solicitudes son aprobadas por: **Aprobación 1** = Dirección de área solicitante.
Nota 2: Las aprobaciones para Trabajo Remoto son realizadas por: **Aprobación 1 =** Dirección del área solicitante, **Aprobación 2** = área de sistemas y **Aprobación 3** = Presidencia.

SISTEMAS

Consecutivo | **Clasificación de la solicitud** | **Tiempo estimado de la solución**

DESCRIPCIÓN DE LA SOLUCIÓN

	Nombre	**Cargo**	**Fecha**
Ejecutado por			

Tabla 10. Formato de Solicitud de Cambios o servicios.
Fuente: Los Autores

1.12 CÓDIGO DE ÉTICA Y CONDUCTA

Objetivo

Este código establece los principios y valores que deben caracterizar a los empleados, clientes y proveedores de Hecc Courrier para el logro de los objetivos en un marco de comportamiento ético dentro de la compañía y que se debe extender a la relación con otras partes interesadas.

Principios o normas de conducta

a. Honestidad
   - ❖ Ser intachable en su proceder.
   - ❖ Utilizar equitativamente los recursos y solo para fines laborales.
   - ❖ Actuar siempre dentro de información objetiva y real, nunca en supuestos no probados o que no se apeguen a la verdad.
   - ❖ No aceptar sobornos ni chantajes.
   - ❖ No realizar acciones censurables o ilícitas para inducir una decisión (por ejemplo, ofrecer dinero para la consecución de un negocio).
   - ❖ Informar o denunciar ante gerencia cualquier suceso del que sea testigo que atente contra el código de ética de Hecc Courrier.
   - ❖ Conducir los negocios con lealtad, claridad, precisión, probidad comercial, seriedad y cumplimiento.
   - ❖ Evitar el surgimiento de conflictos de interés y asegurar un tratamiento equitativo a sus clientes.
   - ❖ Está prohibido utilizar el nombre de Hecc Courrier o sus productos o servicios para actividades particulares.
   - ❖ Está prohibido ofrecer los servicios, experiencia profesional o conocimientos directamente relacionados a la función en Hecc Courrier a clientes o externos a título personal.

b. Respeto
   - ❖ Ser tolerantes con las opiniones de los demás y actuar con prudencia, decoro y seriedad para no ofender a las personas.
   - ❖ Ser amable en el trato con los compañeros de trabajo para mantener la armonía que siempre ha caracterizado el ambiente de trabajo de Hecc Courrier.
   - ❖ Obedecer las reglas y normas de trabajo.
   - ❖ Aceptar la dignidad, creencias, tradiciones, costumbres, diferencias culturales y derechos de las demás personas, sin significar esto que se pueda vulnerar la integridad de los demás y el presente código de ética.
   - ❖ No realizar ningún tipo de acción de maltrato físico y psicológico hacia las demás personas.
   - ❖ No emitir juicios de valor que discriminen.

c. Profesionalismo

   Poner al servicio de Hecc Courrier los conocimientos y experiencias y utilizarlos para enfrentar y solucionar los problemas y requisitos internos y del cliente oportunamente, con claridad, seriedad y probidad.

d. Colaboración

   Disposición para compartir el conocimiento. Para Hecc Courrier es esencial la ayuda, apoyo y asesoría oportuna entre compañeros de trabajo, para garantizar la correcta ejecución de las actividades y el

aprendizaje continuo. Esto lógicamente exige confianza y respeto entre compañeros y disposición de servicio al cliente.

e. Compromiso y Responsabilidad
   - ❖ Cumplir las directrices organizacionales y estratégicas, las normas, acuerdos, procedimientos, instrucciones y en si las disposiciones establecidas y comunicadas por Hecc Courrier a través de cualquiera de los medios de comunicación.
   - ❖ Cumplir a tiempo y satisfactoriamente con las actividades, compromisos y funciones adquiridas.
   - ❖ Asumir con disposición permanente y actitud proactiva los objetivos y metas.

f. Seguridad de la Información
   - ❖ Asegurar que los activos de Hecc Courrier, especialmente la información de clientes y propia de Hecc Courrier, se manejen de acuerdo con los requisitos de confidencialidad, integridad y disponibilidad.
   - ❖ Garantizar que no se ejecutan actividades que incumplan la política de seguridad de la Información.
   - ❖ Generar las actividades laborales, cumpliendo las directrices establecidas y mitigando la probabilidad de generar incidentes de seguridad de la información.
   - ❖ Contribuir a la mejora del Sistema de gestión de la seguridad de la información, comunicando y contribuyendo a la solución de las debilidades encontradas.
   - ❖ Respetar la dignidad y el valor de todas las personas, reconociendo y cumpliendo la normatividad vigente en Colombia sobre protección de datos y sobre el derecho que tienen las personas a la privacidad, confidencialidad, autodeterminación, diversidad y autonomía. Por ende, Hecc Courrier se compromete a respetar y manejar la información de sus empleados conforme a la normatividad en Colombia.

g. Transparencia y Buena Fe
   - ❖ Cumplir los principios constitucionales, legales y los valores éticos en cada una de las acciones.
   - ❖ Mostrar coherencia entre lo que dice y lo que hace.
   - ❖ Reconocer y responder por las consecuencias de las acciones.
   - ❖ Está prohibido solicitar o recibir prebendas o beneficios, dado que esto puede comprometer la objetividad al momento de adoptar una decisión.
   - ❖ No vincular menores de edad. Hecc Courrier está comprometida en la lucha contra el trabajo infantil.

h. Equidad
   Ser transparente, leal y verídico en las decisiones y en la gestión.

Principios De Seguridad

a. Propiedad y Cuidado de los Activos
   Para desarrollar las operaciones requeridas por los clientes bajo las diferentes modalidades de negocio ofrecidas por Hecc Courrier, se manipulan y emplean diferentes tipos de activos: los activos principales tienen un dueño con responsabilidades de imperativo cumplimiento, las cuales incluyen el manejo operativo, condiciones para uso, niveles de protección y custodia. Esta protección se enmarca dentro de los principios de confidencialidad, integridad y disponibilidad de los activos de información.

b. Gestión de la Información
   Para asegurar el cumplimiento de los pilares de seguridad de la información (integridad, confidencialidad y disponibilidad), es preciso cumplir, controlar y mejorar las actividades que conforman el ciclo de vida de la información adquirida o generada por Hecc Courrier, este ciclo incluye las etapas de tratamiento y uso, conservación, hasta su disposición final, lo cual se establece detalladamente en el documento Metodología para el manejo de la información.

c. Confianza
   Asegurar al titular o dueño de información confidencial, que Hecc Courrier toma medidas buscando que su información está protegida en conformidad con las normas de seguridad vigentes legales y contractuales. Por ende, todo empleado de Hecc Courrier está comprometido con el buen uso de los recursos y es consciente de la importancia de la seguridad de la información y la mejora continua en cada una de sus actividades.

d. Continuidad del Negocio
   Implementar, controlar y mejorar el proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información en la organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

1.13 RECOMENDACIONES GENERALES

Principalmente se recomienda ejecutar y cumplir todas las políticas de seguridad establecidas en el presente proyecto, con ello se tiene un sistema de gestión de seguridad de la información capaz de proteger los activos debidamente y hacer que cualquier tipo de riesgo que se pueda presentar se logre mitigar de manera rápida y efectiva con el fin de no perjudicar la continuidad del negocio.

Para tener una seguridad en los sistemas operativos de la organización, se hace recomendación de tener actualizados sus sistemas ya sea Windows (versiones

7 o 10) o Linux con protecciones antivirus, firewalls y demás que logren proteger la información que mantienen tanto en sus ordenadores como servidores. Es clave que el área de sistemas encargada de mantener este nivel de seguridad optimo lo efectúe en todas las áreas de la empresa, además de mantener configuraciones periódicas o actualizaciones que permitan tener una protección de alto nivel en sus activos de software.

En cuanto al software adquirido mediante proveedores de servicios y productos, es claro que en los acuerdos de relación con ellos se establezcan el cumplimiento de las normativas de seguridad y políticas que tienen ambas empresas para que no se vean afectada la información sensible que maneja la empresa Hecc Courrier en sus procesos tanto de envío de correspondencia como los generales de funcionamiento interno. Los proveedores deben estar a cargo de la configuración adecuada y actualización de sus sistemas y desarrollos para que el funcionamiento de la empresa no se vea afectado y la continuidad del negocio prevalezca.

El área operativa y de sistemas debe efectuar controles de funcionamiento en los equipos de infraestructura que se tengan propios de la empresa, ya sean equipos de red, servidores, computadores de escritorio, laptops, servicios de telefonía, equipos de alimentación y suministro de energía, impresoras, etc. Al encontrar fallas de funcionamiento se debe recurrir a la adquisición de nuevos equipos o adquisición de préstamos de equipos por parte de proveedores, donde estos en sus acuerdos de relación con Hecc Courrier se comprometan a tener la instalación, configuración y actualización correcta.

La siguiente lista muestra los equipos necesarios de seguridad para la parte física de la empresa:

- Tarjetas de Aproximación
- Lectores de Tarjetas de Aproximación
- Puertas de seguridad anti-choque
- Cámaras de seguridad para circuito cerrado de vigilancia
- Alarmas contra robo
- Alarmas con monitoreo
- Alarmas contra incendios

Habiendo efectuado revisión de las instalaciones se aconseja modificar el centro de cómputo tanto organizativamente como funcionalmente, ya que se debe escoger un área para un mejor desarrollo y que cuente con equipos de cómputo actualizado para prevenir incidentes de seguridad que se puedan presentar.

Es importante destacar que la red de la empresa debe reestructurarse, tener un cableado estructurado según la norma ANSI/TIA/EIA-568-B, mejores equipos para su funcionamiento como lo son routers, switches, patchpanels, telefonía Ip, etc. Preferiblemente de marcas como Cisco, Intel, Avaya, Broadcom, Atheros, Linksys. De acuerdo a las necesidades que tenga la empresa estos deben ser adquiridos ya sean propios o suministrados por proveedores.