# POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La ESE Hospital Regional del Magdalena Medio del municipio de Barrancabermeja, en cabeza del Gerente, estamos comprometidos con la prestación de servicios de salud y exhibiendo unos altos estándares de calidad, enmarcados dentro de la normatividad que regula el sector y se expide la siguiente Política de Seguridad Informática, dirigida a sus clientes internos y externos:

"Todos los funcionarios, contratistas de la empresa, velarán por el cumplimiento de los procesos y procedimientos estipulados por la empresa para la generación, transmisión, uso, almacenamiento, conservación y divulgación de la información generada, ya sea en forma magnética o física".

Para dar cumplimiento a lo aquí expuesto, la gerencia, a través del Jefe del Subsistema de Información, suscribirá actas de compromiso con los Jefes de las distintas areas, dejando claramente establecidos los mecanismos de seguridad que se emplearán para la custodia y conservación de la información; así mismo, dará a conocer a los clientes externos con los cuales interactúa, los procedimientos necesarios para que la comunicación sea bidireccional y se realice en forma segura.

La alta dirección se compromete también a difundir la presente política a la vez que será estricta en el cumplimiento de las sanciones que se pudieren derivar del mal uso que de la información se pueda hacer.

La ESE Hospital Regional del Magdalena Medio en el presente manual establece otras políticas de seguridad de la información en materia de informática, las cuales se clasifican de la siguiente manera:

## POLÍTICA 1: ACCESO A LA INFORMACIÓN

Todos los funcionarios y contratistas que laboran para la ESE Hospital Regional del Magdalena Medio deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. El área de sistemas del hospital y los responsables de la información deben autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas.

| ELABORADO POR: | REVISADO POR: | APROBADO POR: |
|---|---|---|
| XIOMARA HOYOS BELTRAN | MARTHA E. PRADA LOPEZ | ARMANDO SEGURA EVAN |
| **CARGO:** Jefe Subsistemas de Información | **CARGO:** Subgerente Administrativa y Financiera | **CARGO:** Gerente |

Las claves de acceso compartidas asignadas a los funcionarios de los sistemas información de la Entidad tienen únicamente carácter de consulta, estas no permiten modificación de la información, no deben divulgarse hacia el exterior de la entidad, se cambiarán anualmente o cuando se requiera y exclusivamente se utilizarán para la gestión de la Entidad.

Todos los accesos y claves de usuarios para el uso de los sistemas de información de la entidad, deberán ser desactivados o cambiados después de que un funcionario, deje de prestar sus servicios al hospital.

Mediante el registro del libro de bitácora de auditoría en los diferentes sistemas de información se efectúa un seguimiento a los accesos y cambios realizados por los usuarios a la información del hospital, con el objeto de minimizar el riesgo de pérdida o integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se debe documentar y realizar las acciones tendientes a su solución.

## POLÍTICA 2: ADMINISTRACIÓN DE CAMBIOS

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

## POLÍTICA 3: SEGURIDAD DE LA INFORMACIÓN

Los funcionarios y contratistas de la ESE Hospital Regional del Magdalena Medio son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad y por la Ley para protegerla, evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma. Así mismo no deben suministrar información de la Entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice la infraestructura tecnológica del hospital, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está clasificada como confidencial y/o crítica.

## POLÍTICA 4: SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS

El sistema de correo electrónico, grupos de charla y utilidades deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades del hospital.

Los funcionarios de la ESE Hospital Regional del Magdalena Medio no deben utilizar versiones escaneadas de firmas personales para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmada por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el funcionario se encuentre en el sitio de trabajo, es propiedad exclusiva del hospital. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memorandos, planes, estrategias, productos, software, códigos fuentes, documentación y otros materiales.

## POLÍTICA 5: SEGURIDAD EN RECURSOS INFORMÁTICOS

Los recursos informáticos deben cumplir como mínimo con lo siguiente:

*Administración de usuarios:* Establece cómo deben ser utilizadas las claves de ingreso a los recursos informáticos, longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.

**Rol de Usuario:** Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberá permitir la asignación a cada usuario de diferentes roles, así como existir un rol para la administración de usuarios.

**Registros de auditoría:** Hace referencia a los libros de bitácora de auditoría o registros de los sucesos relativos a la operación.

El control de acceso a todos los sistemas de computación de la Entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras contraseñas o claves de acceso a los recursos informáticos asignados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Toda la información del servidor de la base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de cifrado para garantizar su inutilidad en caso de ser descubierta.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

## POLÍTICA 6: SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser considerados y tratados como información confidencial.

Todas las conexiones a redes externas tiempo real que accedan a la red interna de la Entidad, debe pasar a través de un cortafuegos, denominado sistema de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un documento de formalización.

## POLÍTICA 7: SOFTWARE UTILIZADO

Todo software que utilice la ESE Hospital Regional del Magdalena Medio será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad.

Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios públicos y contratistas de las implicaciones que tiene el instalar software ilegal en los computadores del hospital.

## POLÍTICA 8: ACTUALIZACIÓN DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la Entidad (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas) debe tener previamente una evaluación técnica del área de sistemas, y la autorización del Gerente Administrativo o Financiero o el responsable de los inventarios para la actualización de seriales, responsables y hojas de vida de los equipos.

La reparación técnica de los equipos por la parte externa, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado, previa autorización del Jefe de Subsistema de Información, Gerente Administrativo o Financiero o el responsable de los inventarios.

Los equipos de cómputo (PC, servidores, comunicaciones, etc.) no deben moverse o reubicarse sin la aprobación previa del Jefe de Subsistema de Información, Gerente Administrativo o Financiero o el responsable de los inventarios.

## POLÍTICA 9: ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática de la ESE Hospital Regional del Magdalena Medio deberá ser almacenada y respaldada de tal forma que se garantice su disponibilidad.

El almacenamiento de la información se debe realizar interna y/o externamente a la Entidad, de acuerdo con su importancia.

Los funcionarios públicos son responsables de los respaldos de la información de cada uno de los computadores asignados, de acuerdo con el procedimiento descrito.

La información de copias de seguridad (BACKUP) en CD-R o DVD-R o Discos alternos, debe enviarse al área de sistemas para su custodia, consolidación y archivo.

manipulada por ninguna persona externa o interna durante su transporte y custodia de la misma, estas copias de seguridad permitirán hacer seguimiento de control en una auditoría o en caso de requerirse recuperar la información de los procesos.

## POLÍTICA 10: CONTINGENCIA

El área de sistemas de la ESE Hospital Regional del Magdalena Medio debe preparar, actualizar periódicamente y probar anualmente un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

Las crisis suelen provocar "reacciones de pánico" que pueden ser contraproducentes y a veces incluso más dañinas que las provocadas por el incidente que las causo. Por ello en el presente documento se establece claramente las responsabilidades y funciones del personal así como los protocolos de acción correspondientes.

## POLÍTICA 11: LOG DE AUDITORIA

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Entidad como son los aplicativos en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar un libro con la bitácora de auditoría de la tareas principales (adición, modificación, borrado).

El libro de bitácora de auditoría debe proporcionar suficiente información para apoyar el monitoreo, control y auditorías.

Los archivos de auditoría deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia.

Todos los computadores deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoría sea correcto.

## POLÍTICA 12: SEGURIDAD FÍSICA

La oficinas deben contar con los mecanismos de control de acceso tales como vigilancia privada, identificación de visitantes, sistema de alarmas, etc, y en los sitios donde existan sistemas de información, equipos de cómputo y comunicaciones considerados críticos por la Entidad deben contar mínimo con seguridad de acceso con guardia 7x24x365, sistemas de detección y extinción de incendio, circuito cerrado de televisión con cámaras, redundancia de recursos y alta disponibilidad N+1.

Los visitantes de las oficinas del hospital deben ser escoltados durante todo el tiempo por un funcionario autorizado.

Los centros de cómputo o áreas que la Entidad considere críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente de un funcionario del hospital.

En los centros de cómputo o áreas que el hospital considere críticas deberán existir elementos de control de incendio, inundación, alarmas y estar demarcados como zona restringida. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Los equipos de cómputo (Computadores, servidores, impresoras, equipos de comunicación, entre otros) no deben moverse o reubicarse sin la aprobación previa del Jefe de Subsistema de Información, Gerente Administrativo o Financiero o el responsable de los inventarios.
.
Los funcionarios se comprometen a NO utilizar la red regulada de energía (tomacorrientes naranja o UPS) para conectar equipos eléctricos diferentes a su computador, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que implique una mayor carga sobre esa red.

Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los recursos informáticos de la Entidad.

## POLÍTICA 13: ESCRITORIOS LIMPIOS

Sobre los escritorios u oficinas abiertas y durante la ausencia de los funcionarios del hospital no deben permanecer a la vista documentos en papel, dispositivos de almacenamiento como CDs, memorias USB, con el fin de reducir

los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

## POLÍTICA 14: ADMINISTRACIÓN DE LA SEGURIDAD

Cualquier brecha en la seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, o los recursos informáticos de cualquier nivel (local o institucional) debe ser comunicada por el funcionario que la detecta en forma inmediata y confidencial al área de sistemas del hospital.

Los funcionarios y contratistas que realicen las labores de administración del recurso informático son responsables por la implementación y permanencia de los controles sobre los recursos tecnológicos.

## POLÍTICA 15: PRÁCTICAS DE USO DE INTERNET

Los virus informáticos son una de los principales riesgos de seguridad para los sistemas, por tal razón se deben tomar las siguientes precauciones de seguridad sobre la utilización de Internet:

1. No utilizar canales de chat o grupos sociales como Facebook, Messenger, etc., en horario laboral con fines personales.

2. No descargar de Internet, ni alojar en los discos duros de los equipos de cómputo, música, videos, ni cualquier tipo de software sin licenciamiento.

3. No abrir ningún mensaje, sitio web, ni archivo de fuente desconocida o muy poco conocidas. En caso de personas conocidas, se deben tomar precauciones, asegurándose de que esa persona es la responsable del envío y ante cualquier duda, borrar el mensaje, para evitar la contaminación de un virus.

4. Todos los funcionarios del hospital, tienen la obligación a dar cumplimiento a la Ley 679 de 2001, acatando las prohibiciones que le han sido impuestas. Por consiguiente se obligan a no utilizar los servicios, redes y sistemas del hospital que impliquen directa o indirectamente, bajar o consultar información de actividades sexuales y/o material pornográfico.

5. El spam o correo basura son los mensajes no deseados que hacen referencia a publicidad pudiendo además contener virus; estos mensajes deben

eliminarse sin ser leídos para evitar el aumento de la cantidad del correo basura en el buzón así como la posibilidad de intrusión de virus en el sistema.

6. Usar regularmente un programa antivirus y verificar periódicamente su actualización, el área de sistemas presta el soporte que se requiera para tal fin.

7. No bajar nada de sitios web de los que no se tenga referencias de seriedad, o que no sean medianamente conocidos. Si se bajan archivos, copiarlos a una carpeta y revisarlos con un antivirus actualizado antes de abrirlos.

8. Se debe suministrar el correo electrónico asignado por el hospital con moderación, ya que podrían enviar publicidad no deseada.

9. No utilizar la cuenta de correo electrónico suministrada por el hospital, para asuntos personales.