HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

IBAGUE 2019

Calle 33ª 4-A 50 Tel. 2648979- 2640888 extensión 209 Web Site: www.hflleras.gov.co
E-mail.hflleras@hflleras.gov.co. Sistemas de Información

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

"La información generada en la institución en el desarrollo y cumplimiento de los procesos procedimientos y tareas, debe cumplir con todos los lineamientos y controles funcionales de procesamiento, análisis, confidencialidad, accesibilidad y seguridad."

INTRODUCCIÓN

Con base en el trabajo realizado por los integrantes del **Grupo Operativo de Gobierno Digital y Seguridad de la Información**, se organizó la política de Seguridad y Privacidad de la Información, herramienta base para contar con los lineamientos y controles para garantizar la seguridad y privacidad de la Información.

La seguridad física identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen el hardware, el software y las redes de datos, los medios de almacenamiento de datos, y los demás componentes informáticos. En general los activos asociados al almacenamiento, procesamiento y salida de la información.

OBJETIVOS

GENERAL

Cumplir con todos los lineamientos y controles funcionales de procesamiento, análisis, confidencialidad, accesibilidad y seguridad de la información generada por la institución

ESPECIFICOS

- Establecer los lineamientos y controles para el uso de los recursos informáticos de la institución garantizando la seguridad de los mismos.
- Determinar los niveles de acceso a las Aplicaciones en Producción que se ejecutan en la institución para el almacenamiento, procesamiento y salida de los datos, conforme a los ROLES, PERFILES Y PERMISOS.
- Establecer los parámetros para la administración de la red LAN EXTENDIDA del Hospital, mediante la actualización de la documentación del direccionamiento IP y el establecimiento de las VLANS y LOS GRUPOS VIRTUALES.
- Determinar los parámetros de validación de las copias de seguridad de los datos BACKUP Y RESTORE, conforme con el Instructivo GA-IN-008-RESPALDO DE DATOS A APLICACIONES EN PRODUCCIÓN.
- Administrar los grupos Virtuales, de acuerdo con los niveles de acceso a internet de acuerdo al requerimiento por procesos y procedimientos que requieren,
- Definir los controles para el acceso a servidores de la Institución y la bitácora de los procesos que se ejecutan directamente en la infraestructura y los puertos para el acceso a los recursos.

1. AREAS DE TECNOLOGIA DE LA INFORMACIÓN

Se entiende por AREAS DE TECNOLOGIA DE LA INFORMACIÓN donde se procesa la información:

- DATA CENTER

  Área en donde se encuentran instaladas las Infraestructura de Servidores

- Áreas donde se encuentren concentrados dispositivos para la interconexión de estaciones de trabajo de la Red "Racks" o Centrales de Cableado

- Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos Duros, USB, Cintas Magnéticas, etc.)

- Oficina de Tecnología de la Información

1.1 Activos informáticos

Activos Informáticos: Corresponde a elementos tales como bases de datos, documentación, manuales de usuarios, planes de contingencia, Plan de Recuperación del Sistema, entre otros.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, motores de base de datos, Sistemas Operativos; en general todo lo relacionado con el software y las licencias de Software.

Activos físicos: Se consideran activos físicos elementos tales como: Servidores, Computadores, laptops, módems, impresoras, Equipos de Comunicaciones, PBX, cintas, discos, USB , UPS, etc. Es decir lo relacionado con el hardware y Sistemas ininterrumpidos de Potencias Regulados por UPS.

1.3 Elementos de la política de Seguridad y Privacidad de la información

Aspectos de la seguridad física a ser considerados en la definición de las políticas funcionales:

- Procesos y procedimientos
- Servidores Físicos
- Servidores Virtuales
- Estaciones de trabajo
- Impresoras y Scanners
- Herramientas de Respaldo y Recuperación de Datos
- Medios de almacenamiento de datos
- Cableado Estructurado
- Sistemas Ininterrumpido de potencia (UPS)
- Sistema de seguridad (firewall)
- Componentes y recursos de acceso remoto
- Documentos restringidos
- Datos e Información

1.4 Políticas relacionadas

- Política de Control de Acceso del personal a la institución.

1.5 Roles y responsabilidades

Esta política es responsabilidad de la Gerencia de la Información o quien haga sus veces, con el fin de garantizar el buen uso y la Seguridad de los recursos informáticos de la institución.

1.6 Violaciones a la política de Seguridad y Privacidad de la Información

La violación de la política de Seguridad Física, pueden resultar en acciones de tipo disciplinario, más no estar limitadas a:

- Acción de tipo disciplinario según los lineamientos establecidos por el Código Sustantivo del Trabajo, el Reglamento Interno de Trabajo, y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias patronales

1.7 Revisión de la política de Seguridad y Privacidad de la información

Esta política para que sea modificada debe ser aprobada por la Gerencia del Hospital Federico Lleras Acosta de Ibagué E-S-E. Cuando quede corta frente al avance tecnológico o cambio de infraestructura de la organización.

2. ASPECTOS ESPECÍFICOS SOBRE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El sitio escogido para instalar estaciones de trabajo o equipos de cómputo y comunicaciones, deben cumplir con los requerimientos que garanticen las seguridad de los mismos frente a daños o accesos no autorizados.

2.1 Recomendaciones y controles adicionales

El tamaño del área será determinado por la cantidad de hardware necesitado para el procesamiento y almacenamiento de la información. Los requerimientos de tipo ambiental deben ser especificados por los diferentes fabricantes de los equipos. Las medidas de seguridad que se deban tomar, dependerán directamente del valor de los activos de información y su nivel de confidencialidad.

2.2 Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas:

- El sitio donde se ubiquen los recursos informáticos debe ser físicamente sólido, y protegido de accesos no autorizados,
- Debe existir un área de recepción que solo permita la entrada de personal autorizado a las áreas restringidas
- Todas las salidas de emergencia en el perímetro de seguridad deben tener alarmas sonoras y cierre automático.

2.3 CONTROL DE ACCESO FÍSICO

Control a todos los sitios en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas.

Se recomienda además tener separados físicamente la operación de terceros con las propias, en caso de existir actividades de terceros en HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E, se deben establecer controles por la persona responsable en EL HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E, y del Outsourcing si es el caso.

2.3.1 Recomendaciones y controles Adicionales

Debido al posible robo, vandalismo y uso no autorizado de los recursos de información, se debe considerar restringir el acceso de personas a las áreas restringidas, según lo definido por HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E.

Todo sistema de control de acceso debe considerar diferentes categorías de personal:

1) Operadores y usuarios que trabajan regularmente en las áreas restringidas.
2) Personal de soporte que requiera acceso periódico.
3) Otros, que requieran acceder esporádicamente (auditores, revisores).

2.3.2 Aspectos de la seguridad de la información a ser considerados cuando se implementa la política de seguridad física son:

- El Personal del HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E, visitantes o terceras personas, que ingresen a un área definida como restringida por la Institución, deberán poseer una identificación a la vista que claramente los identifique como tal y estas identificaciones serán intransferibles. Se debe además hacer una revisión periódica de identificadores de acceso; una formal realizada con auditoria al menos una

vez al año, y en las diferentes divisiones internamente realizarlas cada 3 meses.

- En caso de pérdidas de llaves, deberán existir procedimientos que garanticen que las mismas no podrán ser utilizadas por extraños.

- Los equipos de, fotocopiadoras, impresoras deben estar en áreas definidas por HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E como seguras, esto aplica también para equipos de comunicaciones como Switches, Enrutadores, firewalls, VPN, etc.

- Las puertas y ventanas del centro de cómputo deben estar cerradas, en caso de ser el primer piso se deben considerar controles adicionales **"frente** a **riegos naturales y ocasionados por el hombre"**

2.5 Uso de impresoras

La información clasificada como altamente confidencial no debe ser enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión. La variedad de la información que se envía a las impresoras puede alternar entre información pública e información confidencial, dado que información confidencial puede ser revelada a personas no autorizadas.

2.6 Presencia de extraños en las instalaciones Hospital Federico LLeras Acosta de Ibagué E-S-E.

Todos los empleados deben estar vigilantes a la presencia de personas extrañas sin identificación visible dentro de las instalaciones Restringidas del HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E y en ese caso reportar inmediatamente a seguridad.

Entre los controles adicionales tenemos:

- Todos los visitantes o extraños deben ser acompañados durante su estadía en HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E, en las áreas restringidas, debido a la existencia de información confidencial o hurto.

- Equipos como videograbadoras, cámaras fotográficas, grabadoras y medios de almacenamiento de datos, (USB, CD, DVD Y DISCOS FLEXIBLES ENTRE OTROS) etc., no deben ser permitidos su uso dentro de las instalaciones de HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E a menos que exista un registro formal por la persona responsable de la Unidad Funcional.

2.6.1 Descargue de equipos de cómputo

- Todo elemento que ingrese a HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E, debe ser inspeccionado por la compañía de Vigilancia rigurosamente, con el fin de identificar material peligroso y que coincida con su respetiva autorización de ingreso.

- El equipo entrante o saliente debe ser registrado por el personal de vigilancia de la Institución, en el formato respectivo.

2.7 Seguridad de los equipos

En lo referente a la ubicación de computadores y hardware en general, se debe tener especial cuidado contra fallas del sistema de control del medio ambiente, y otras amenazas que puedan afectar la normal operación del sistema.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- Fallas en el control de la temperatura o humedad pueden afectar la operación del sistema, así que, se debe tener un estricto monitoreo sobre estas variables.

- Se deben adoptar o mantener al día, controles para minimizar el riesgo potencial de:

- Robo.

- Todos los visitantes o terceras personas, que ingresen a las instalaciones de HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E deberán poseer una identificación a la vista que claramente los identifique como tal.

- En el Data Center, deben de existir detectores de temperatura y humo, instalados en forma adecuada para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante y al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos del de la Oficina de la Oficina.

- Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales y garantizar que el personal del área conoce sobre el manejo de los mismos.

- Todos los visitantes o terceras personas, que ingresen a un área de procesamiento deberán poseer una identificación a la vista que claramente los identifique como tal, y por ninguna razón se debe tener material explosivo dentro, o en sitio cercano a áreas definidas como restringidas por HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E. (Por ejemplo químicos especiales, pólvora o gases explosivos)

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan. Cumpliendo con las normas de cableado estructurado **EIA 568 A - EIA 568B**.

- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

- Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, ni tomar ningún tipo de bebidas o consumir alimentos.

- Los equipos deben ser protegidos de fallas de potencia u otras anomalías de tipo eléctrico. Los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes de los equipos.

- El correcto uso de UPS (Uninterruptible Power Supply), las cuales se deben probar según las recomendaciones del fabricante, de tal forma que

garanticen el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.

2.8 Instalación y mantenimiento del cableado

- El cableado estructurado debe ser instalado y mantenido, con el fin de garantizar su integridad. Conectores de pared no utilizados deben ser sellados y su estado debe ser formalmente notificado.
- Las conexiones de potencia deben tener su respectivo polo a tierra.
- El cableado de la red debe ser protegido de intercepción o daño, por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de acuerdo a las normas técnicas, de los de comunicaciones.
- Para el caso de conexiones muy críticas (Transporte de mucha información o aplicaciones especiales) se debe considerar el uso de fibra óptica. Considerar el uso de enlaces redundantes.

3 MANTENIMIENTO DE LOS EQUIPOS

Se deberán realizar mantenimientos a los equipos de acuerdo a las recomendaciones del fabricante y ser realizados únicamente por personal autorizado, considerando el hecho que si se tuviera que enviar fuera de las instalaciones, se debe tener en cuenta la información sensitiva y los requerimientos de las pólizas de aseguramiento.

3.1 Equipos fuera de las instalaciones

El uso de equipos de procesamiento de la información o software, fuera de las instalaciones del HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E, debe ser autorizado por el jefe o director del área donde el empleado dependa.

Esto aplica para Computadores personales, agendas electrónicas, teléfonos móviles, etc.

Las siguientes recomendaciones deben ser consideradas:

- El trabajo remoto debe estar sujeto a controles especiales, considerando las recomendaciones aplicadas cuando su uso es de tipo interno.

3.2 Política de escritorios y pantalla

EL HOSPITAL FEDERICO LLERAS ACOSTA DE IBAGUE E-S-E debe adoptar la medida de escritorios limpios de papeles, y medios de información, junto con una medida de pantalla limpia, con el fin de reducir los riesgos por pérdida, daño a la información durante o fuera de las horas de trabajo.

Los siguientes controles deben ser considerados:

- La información confidencial y crítica para la organización debe ser asegurada preferiblemente en armarios resistentes a impacto, fuego e inundación

- Los computadores personales no se deben dejar dentro de sesión, se recomienda el uso de llaves físicas, contraseñas, y otro tipo de controles cuando no estén en uso.

- Las fotocopiadoras deben estar protegidas de uso no autorizado.

3.3. Creación de cuentas de acceso a la red y a las Aplicaciones en Producción.

- Cuando el usuario de la red y de aplicativos sea desvinculado de la institución, el jefe inmediato debe de Solicitar la cancelación de las cuentas de acceso, a la Oficina de Tecnología de la Información del sistema conforme al procedimiento y formato respectivo.

- Las contraseñas utilizadas para el proceso de autenticación deben ser cambiadas periódicamente y se debe de utilizar la combinación de Números, Letras Mayúsculas, Letras Minúsculas y Caracteres Especiales.

- La contraseña es personal e intransferible.

4. ACCESO REMOTO

De acuerdo a la necesidad y el manejo de información se deben establecer los procesos para el acceso remoto a los recursos disponibles de la institución.

4.1 **Usuario interno por acceso remoto por el protocolo de comunicación MSTSC**

Conforme a los perfiles y permisos establecidos por la Oficina de Tecnología de la Información

4.2 **Usuario Externo por VPN**

4.2.1 Soporte a aplicaciones, Implementación de aplicaciones y monitoreo de la base de datos conforme al **GA-IN-010- SOPORTE Y ADMINISTRACION DE INFRAESTRUCTURA**

5. CONTROL DEL CONTENIDO WEB

El contenido de la Plataforma Web del Hospital, está regulado por la Oficina Asesora de Planeación y Calidad del Hospital Federico Lleras Acosta de Ibagué E-S-E.

- 5.1 Aprobar la documentación a publicar en la Intranet del Hospital www.hflleras.gov.co\intranet
- 5.2 Están definidas las Oficinas o Unidades Funcionales que pueden publicar en el Web Site: www.hflleras.gov.co

GLOSARIO

CIBERSEGURIDAD:

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701). • Ciberespacio Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).

CIBERESPACIO:

Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).

AUTENTICACIÓN:

Un método sistemático para verificar la identidad de un usuario.

AUTORIZACIÓN: Un procedimiento por el cual se otorgan permisos a alguien en relación a un sistema.

BASTIÓN DE SERVIDORES: Donde servidores de uso crítico pueden ser alojados, y alrededor de los cuales se implementan políticas adecuadas de seguridad lógica y física.

CAPACIDAD DE RESPUESTA A INCIDENTES: Es el conjunto de habilidades para responder de forma adecuada y eficaz a cualquier incidente que comprometa la seguridad de los recursos de información y comunicaciones.

CONFIDENCIALIDAD: Atributo de la información almacenada en un sistema por el cual, por tratarse de datos privados o sensibles, puede causar perjuicios si es accedida o publicada por agentes sin autorización.

CONTROL DE ACCESO: Un medio físico y/o electrónico que asegura que solamente quienes estén autorizados para visualizar, actualizar, corregir y/o borrar los datos en un sistema puedan acceder a tales recursos.

DESENCRIPCIÓN: Procedimiento de transformar en legible un texto inicialmente cifrado.

DISPONIBILIDAD: la certeza que un sistema de información sea accesible por los usuarios autorizados cada vez que sea necesario o que esté programado o predefinido.

ENCRIPCIÓN: Procedimiento para transformar un texto legible en otro cifrado no legible.

FILTROS (CORTAFUEGOS O FIREWALLS): Sistemas de filtros basados en políticas adoptadas, que controlan y restringen el tráfico de datos entre computadoras en red. Los firewalls establecen un perímetro físico o lógico donde tipos de tráfico preseleccionados se bloquean por razones de seguridad. Las políticas de bloqueo se pueden basar en direcciones IP o en el tipo de protocolo de aplicación. En la presente política se incluyen diferentes clases de firewall:

- Firewalls integrados en Sistemas Operativos.
- Firewalls dedicados para proteger laboratorios o grupos de servidores.
- Firewalls dedicados a proteger equipos individuales.

COMPUTACION FORENSE: La disciplina encargada de analizar los medios de almacenamiento de computadoras, archivos de auditoría, o cualquier otro recurso de computación con el fin de encontrar evidencia de delitos mediante computadoras u otra clase de violaciones.

INCIDENTE DE SEGURIDAD: Cualquier evento durante el cual algún aspecto de la seguridad de una computadora es afectado.

INTEGRIDAD: Calidad de los sistemas o de los datos contenidos en ellos de permanecer intactos, inalterables y confiables.

MANEJO O CONTROL DE RIESGOS: Una metodología razonable que pretende alcanzar un balance riesgos-beneficios en un ambiente o sistema determinado.

NO-REPUDIO: Un procedimiento o acción de mutuo consentimiento entre el emisor y el receptor de un mensaje sobre la autenticidad de la información transferida, o cualquier método operativo que provea pruebas en cuanto a la

identidad de los emisores/receptores en una transacción electrónica u otra actividad equivalente.

OPERADORES DE SISTEMAS: personal del PED, quienes están a cargo de las decisiones y acciones operacionales en cuanto al uso y administración de un sistema de cómputos, bajo la coordinación o supervisión de los correspondientes Administradores.

PERÍMETRO DE SEGURIDAD: Conjunto de habilidades o medios destinados a proteger los límites exteriores de una red, de un área física o lógica.

PRINCIPIO DEL PRIVILEGIO MÍNIMO: Principio que establece que los privilegios de acceso a sistemas para cualquier usuario deben limitarse sólo a lo necesario para completar las tareas o funciones asignadas, y no exceder de tal posibilidad.

PRIVACIDAD: Derecho del individuo a ser dejado sólo, apartado de las influencias de su entorno y a estar protegido contra el mal uso o abuso de las cosas que pertenecen legalmente al individuo y que son consideradas por el encuadre legal como de su propiedad.

SEGURIDAD: Un atributo de los sistemas de información que incluye procedimientos y recursos específicos basados en políticas con el objeto de proteger la confidencialidad y la integridad de la información, la disponibilidad y funcionalidad de los servicios críticos, y la privacidad de los individuos.

USUARIOS: Cualquier individuo que tenga privilegios o accesos aprobados por las autoridades competentes para ingresar o utilizar los recursos de cómputos o servicios de redes, aplicaciones e información.

INTRANET: Una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales. El término intranet se utiliza en oposición a *Internet*, una red entre organizaciones, haciendo referencia por contra a una red comprendida en el ámbito de una organización.

EDGAR VARGAS MATEUS
Profesional – Universitario – Tecnología de la Información