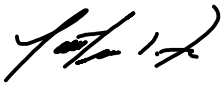
# MANUAL PARA LA GESTIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN.

| | ELABORADO POR | REVISADO POR | APROBADO POR |
|---|---|---|---|
| CARGO | LIDER DE GSTION DE LA INFORMACION | SUBGERENTE ADMINISTRATIVA | GERENTE |
| NOMBRE | EMERSON GONZALEZ | YANNETH LUCIA VILLAE | LIFAN MAURICIO CAMACHO |
| FIRMA |  |  |  |
| FECHA | 17 DE DICIEMBRE 2020 | 21 DE DICIEMBRE 2020 | 29 DE DICIEMBRE DE 2020 |

| CONTROL DE CAMBIOS | | |
|---|---|---|
| VERSIÓN No | FECHA DE APROBACIÓN | DESCRIPCIÓN DEL CAMBIO |
| 00 | 29 DE DICIEMEBRE 2020 | NORMALIZACION MANUAL PARA LA GESTION DE LA POLITICA DE SEGURIDAD DE LA INFORMACION |

MANUAL PARA LA GESTIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

## Contenido

## 1. OBJETIVO

Establecer los lineamientos de seguridad enmarcados dentro de la política de Gobierno Digital y la política de seguridad, privacidad de la información y seguridad digital.

## 2. ALCANCE

Este manual Contempla los lineamientos de la estrategia de gobierno en digital y los lineamientos principales para la seguridad de la información de la E.S.E. Hospital Regional de Duitama, los cuales deben ser conocidos y apropiados por usuarios, pacientes, colaboradores, empleados, demás partes interesadas y la ciudadanía en generalque tenga acceso, almacene, procese o trasmita información de la E.S.E. Hospital Regional de Duitama.

## 3. MARCO LEGAL APLICABLE

Ley Estatutaria 1581 de 2012: y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 2578 de 2012: Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye “El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles” entre otras disposiciones.

Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.
Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. "Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Norma ISO 27001: Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.

## 4. RESPONSABLE

El proceso de Gestión de la información será el responsable del cumplimiento de estas directrices.

## 5. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de información:** Los activos de información son el resultado de la construcción de un inventario y clasificación de los activos que posee la entidad de acuerdo con la Política General de Seguridad y Privacidad de la información, la cual determina que activos posee la entidad, cómo deben ser utilizados, así como los roles y responsabilidades que tienen los funcionarios sobre los mismos. 1 En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el

[1] https://www.mintic.gov.co/portal/inicio/101640:10-6-Activos-de-informacion

transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **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:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- **Control:** Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales

debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Disponibilidad:** Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan.
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Evento de seguridad de la información:** Es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Guía:** Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Incidente de seguridad de la información:** Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de

comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Parte interesada:** (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Propietario/responsable de activo de información:** Individuo, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
- **Política:** Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.

- **Procedimiento:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Servicio:** Es cualquier acto o desempeño que una persona puede ofrecer a otra que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Usuario:** Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es única en cada servidor, y cada usuario tiene asignado una contraseña para poder acceder a su cuenta.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

## 6. SEGURIDAD DEL RECURSO HUMANO

Todos los usuarios, colaboradores, empleados, demás partes interesadas y la ciudadanía en general de la E.S.E Hospital Regional de Duitama, que tengan la posibilidad de acceder a la información de la Institución o a la infraestructura tecnológica para su procesamiento, almacenamiento o consulta, son responsables de conocer, acatar y poner en práctica las políticas institucionales establecidas para el manejo de seguridad, privacidad de la información y seguridad digital. Adicionalmente serán responsables por la información reportada a terceros, partes interesadas y ciudadanía en general por cualquier medio sea este físico o electrónico.

Todos los usuarios, colaboradores y empleados de la E.S.E. Hospital Regional de Duitama, deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones, en redes sociales, foros o chats o situaciones que pongan en riesgo la seguridad y el buen nombre de la Institución, así como de pacientes, usuarios, colaboradores o empleados.

### 6.1 Roles y responsabilidades

El proceso de Gestión del Talento Humano será el encargado de diseñar, documentar y actualizar el manual especifico de funciones y requisitos por competencias laborales, para los empleos que conforman la planta de personal de la E.S.E. Hospital Regional de Duitama, donde se detallan los roles, las responsabilidades, funciones o actividades a ser ejecutadas.

Para los contratistas y/o terceros se describirán las responsabilidades y actividades en los contratos respectivos que intervienen con la Institución.

Todo el personal, contratista y/o tercero definido por la E.S.E. Hospital Regional de Duitama, deben regirse a las políticas de Seguridad de la Información, así como los términos de uso adecuado de los recursos de información que le son entregados, responsabilidades extensibles aún fuera de la Institución.

Todo el personal, contratista y/o tercero que tengan acceso a información sensible de la Institución o a la Infraestructura tecnológica, debe firmar, previamente a la entrega del acceso, un acuerdo de confidencialidad y no divulgación, en el que se especifique el período por el cual debe mantener el acuerdo y las acciones que se toman cuando se incumpla este requerimiento. Incluye aspectos como propiedad intelectual, protección de

la información, leyes aplicables basados en las Políticas Institucionales, Políticas de Seguridad de la Información, Políticas de tratamiento protección de datos personales.

### 6.2 Plan de sensibilización, capacitación y comunicación sobre la seguridad de la información.

La E.S.E. Hospital Regional de Duitama, deberá asegurar que todo el personal, contratista y/o tercero que tengan acceso a información tenga claramente definidas las responsabilidades en de Seguridad de la Información y los riesgos conocidos a los que se puede ser expuesta, en caso de que estas no se cumplan a cabalidad, que son competentes para desempeñar sus funciones y que cuentan con los programas de capacitación y entrenamiento requeridos para ello.

Los programas de sensibilización, capacitación y comunicación, se encuentran diseñados y actualizados continuamente de manera apropiada y relevante para los roles, responsabilidades y habilidades de las personas que deben asistir a ellos.

### 6.3 Proceso disciplinario

La Gerencia debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente en el hospital, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo amerita.

### 6.4 Terminación o cambio de la contratación laboral o cambio de funciones

La oficina de talento humano independiente del tipo de vinculación del personal será la encargadas de informar a las áreas implicadas en los procesos de vinculación y desvinculación, los movimientos del personal, contratista y/o tercero según los lineamientos establecidos en la E.S.E Hospital Regional de Duitama.

La Subgerencia Administrativa, Subgerencia Científica, la oficina de talento humano y la oficina de gestión de la información, en conjunto con el jefe directo del funcionario y/o responsable del tercero, son los encargados del proceso de terminación de labores y asegurar que todos los activos propios de la Institución sean devueltos, los accesos físicos y lógicos sean eliminados, y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos en el proceso de terminación de contrato. Este mismo procedimiento deberá ser implementado en el caso de que el funcionario y/o tercero cambie de funciones o asignaciones y asegurar la entrega tanto de activos como accesos físicos y lógicos y la transferencia de la información.

## 7 GESTION DE ACTIVOS

Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas de la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Para garantizar su administración y control la oficina de Gestión de la Información mantendrá un inventario actualizado con las respectivas hojas de vida en el aplicativo PACH institucional junto con el cronograma de mantenimiento preventivo de estos activos. En el caso de realizar traslados de equipos, reubicaciones estas serán informadas a través del correo electrónico institucional a la oficina de almacén quien a su vez realizara el control en el inventario de activos fijos en el sistema de información Dinámica Gerencial Hospitalario (DGH).

### 7.1 Asignación de Activos

La Subgerencia Administrativa, el almacenista y los líderes de procesos serán los encargados de identificar al funcionario y/o terceros responsables de los activos quienes deberían garantizar el uso y protección adecuada de los activos, la información adquirida o procesada en ellos.

### 7.2 Devolución de activos

Todo el personal, contratista y/o tercero de la E.S.E Hospital Regional de Duitama al momento de su retiro o cambio de funciones deberá hacer entrega de los activos junto con un inventario detallado de la información contenida en ellos.

### 7.3 Traslado de activos

Para el traslado de activos tecnológicos debe realizarse la solicitud a través de la aplicación institucional PACH para que la oficina de gestión de la información realice el trámite correspondiente.

### 7.4 Clasificación de la información

El comité institucional de gestión y desempeño el responsable de clasificar la información en términos de su valor, requerimientos legales, y grado crítico para la organización, la información se va a evaluar y definir de acuerdo a las tres características en la cuales se basa la seguridad:

**a) Confidencialidad:**

a. PÚBLICO: Información que puede ser conocida y utilizada sin autorización por

cualquier persona, sea empleado de la entidad o no.

b. RESERVADA –USO INTERNO: Información que puede ser conocida y utilizada por todos los empleados de la entidad y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, el Sector Público Nacional o terceros.
c. RESERVADA -CONFIDENCIAL: Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la entidad, al Sector Público Nacional o a terceros.
d. RESERVADA SECRETA: Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, de nivel directivo de la entidad, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves, al Sector Público Nacional o a terceros.

**b) Integridad**

a. **0-**Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación de la entidad.
b. **1-**Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para la entidad, el Sector Público Nacional o terceros.
c. **2-**Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la entidad, el Sector Público Nacional o terceros.
d. **3-**Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la entidad, al Sector Público Nacional o a terceros.

**c) Disponibilidad**

La inaccesibilidad a la información puede:

a) **0-**La inaccesibilidad a la información a no afecta
b) **1-**La inaccesibilidad a la información durante un periodo de tiempo no menor a una semana podría causar pérdidas significativas
c) **2-**La inaccesibilidad a la información durante un periodo de tiempo no menor a un día podría causar pérdidas significativas
d) **3-**La inaccesibilidad a la información durante un periodo de tiempo no menor a una hora podría causar pérdidas significativas

## 8 POLITICAS DE CONTROL DE ACCESO

Limitar el acceso a información y a instalaciones de procesamiento de información. La Oficina de gestión de la información, como responsables de las redes de datos y los recursos

de red del hospital, debe propender porque dichas redes el sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

### 8.1 Política de administración de acceso de red de datos

- Le corresponde a la oficina de gestión de la información la administración de la red de datos y los recursos de red, también debe garantizar que dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.
- La oficina de gestión de la información debe autorizar la creación o modificación de las cuentas de acceso a la red de datos del hospital, y sus sedes integradas en red.
- La oficina de gestión de la información debe establecer un procedimiento de control de acceso a la red de datos físicas e inalámbricas utilizando el servidor DHCP, el Firewall y la VPN con los que cuenta la institución garantizando que solo los equipos autorizados puedan acceder a los recursos en red.
- La Oficina de gestión de la información debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- Los equipos de cómputo asignados a usuarios finales incluyendo el personal provisto por terceros, que se conectan por primera vez a la red de datos del Hospital, deben contar con la aprobación de la oficina de gestión de la información, y únicamente podrán realizar tareas para los que fueron autorizados
-

### 8.1 Política de administración de acceso a usuarios

- La oficina de gestión de la información debe establecer un procedimiento formal para la administración de usuarios en la red de datos, los recursos tecnológicos y sistemas de información de la institución, que contemple la creación, modificación, y bloqueo de las cuentas de usuario.
- La oficina de gestión de la información, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y el sistema de información de la E.S.E Hospital Regional de Duitama y sus sedes integradas en red; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación, entre otros.
- La oficina de gestión de la información, previa solicitud de la oficina de talento humano debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información

administrados, acorde con el procedimiento establecido.

- La oficina de gestión de la información, debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
- La oficina de gestión de la información debe descontinuar o modificar de manera inmediata los privilegios de acceso lógico al sistema de información, sistema operativo, y demás sistemas que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

## 9 POLITICAS DE SEGURIDAD FISICA Y DEL ENTORNO

### 9.1 Áreas seguras

Se establece como área segura el denominado DATACENTER del segundo piso del edifico administrativo de la sede de Duitama, donde se realiza el procesamiento y almacenamiento de información, así como los centros de datos de imágenes diagnosticas, centros de cableado oficina de gestión de la información y los centros de datos y cableado de cada una de las sedes integradas en red. Los centros de procesamiento y almacenamiento de información deben contar con protección contra incendios.

### 9.1 Controles físicos de ingreso

- El acceso a las áreas de procesamiento y almacenamiento de información sensible tales como DATACENTER, centros de cableado, oficina de gestión de la información deben estar protegidos por puertas metálicas.
- El acceso a las áreas de procesamiento y almacenamiento de información (DATACENTER-OFICINA DE GESTIÓN DE INFORMACIÓN-SERVIDORES DE IMÁGENES DIAGNOSTICAS) debe estar protegida mediante control biométrico de acceso con registro de fecha y hora de acceso de los funcionarios autorizados.

## 10 POLITICA DE SEGURIDAD DE LAS OPERACIONES

La oficina de gestión de la información es la encargada de garantizar la operación y administración de los recursos tecnológicos de la entidad por lo cual deberá asignar a sus funcionarios funciones específicas para la operación, mantenimiento actualización y documentación de los procesos operativos. Adicionalmente velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la

información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

### 10.1 Política contra software malicioso

- Se adquirirá y utilizará software únicamente de fuentes confiables, en caso de ser necesaria la adquisición de software de origen no confiable, este se debe adquirir en código fuente.
- La oficina de gestión de la información debe asegurarse que el servidor, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.
- La oficina de gestión de la información debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la oficina de gestión de la información; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

### 10.1 Políticas para copias de respaldo

El objetivo de esta política es asegurar la generación de copias de respaldo de los datos y software de la E.S.E Hospital regional de Duitama, asignando los roles, recursos y medios necesarios, estableciendo lineamientos de respaldo y almacenamiento de la información.

- El líder de proceso o responsable de la información de cada procedimiento será el responsable de identificar y conservar actualizados los **activos de información**.
- Para cada copia de respaldo, se deberá considerar la frecuencia, los medios de almacenamiento, tipo de contenido, tiempo de almacenamiento y borrado de esta información.
- La periodicidad con que se realizarán los respaldos de los computadores portatiles o estaciones de trabajo de la entidad deberá ser mínimo de 1 respaldo anual, esta información es la que cada persona reporta a la oficina de gestión de la información y es responsabilidad de cada colaborador.
- Todas las áreas que generan información deberán definir la frecuencia del respaldo de esta e informarle a la oficina de gestión de la información, esta información se debe

diligenciar en la matriz de activos de información.

- Los medios de respaldo que contienen información deben tener una custodia que garanticen la protección adecuada de los datos allí almacenados, de forma que cumplan con los requisitos para ser puestos en funcionamiento en cualquier momento que sea requerido, además se deberá tener las copias de seguridad en un lugar secundario para mitigar riesgos en caso de un evento inesperado dentro de los sitios donde se generan las copias de respaldo.
- Ante un cambio tecnológico que se produzca que pueda generar obsolescencia tecnológica, deben generarse las acciones necesarias de resguardo de la información de los medios de respaldo.
- Deberán existir registros documentados de las copias de respaldo y del restablecimiento de estas.
- El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado.
- Toda información crítica grabada en medios de respaldo que son almacenados fuera de la entidad deberá ser trasladada con los elementos de seguridad adecuados, como por ejemplo el uso de controles criptográficos.
- Cada líder de proceso deberá determinar el período de conservación del respaldo de la información crítica de sus procesos, teniendo en cuenta los requisitos de conservación de las tablas de retención documental, la normativa legal vigente, el uso eficiente del espacio físico y los medios de almacenamiento disponibles.
- La oficina de gestión de la información deberá considerar, dentro de sus recursos asignados, soluciones de respaldo para equipos de escritorio. Siendo los usuarios de la entidad los responsables de alojar la información propia de su objeto contractual que necesita ser respaldada en los lugares establecidos para ello. No se respaldará información personal del usuario ya que en los computadores suministrados por la entidad no está autorizado el almacenamiento de este tipo de información.
- Se deberán utilizar los medios que la oficina de gestión de la información disponga para realizar las copias de respaldo.
- La oficina de gestión de la información deberá asegurarse de que la información del objeto contractual del personal de la entidad sea salvaguardada de forma satisfactoria.
- La ejecución de las pruebas de restauración de las copias de respaldo deberá asegurar la recuperación de copias de datos, y garantizar la integridad de los datos que contienen.
- Se deberán realizar pruebas respecto a la restauración de las copias de respaldo en forma controlada y en un ambiente seguro que contenga los mismos niveles de seguridad del ambiente original, de forma rotativa y con una periodicidad de mínimo 1 vez por año.

## 11 POLITICA DE SEGURIDAD DE LAS COMUNICACIONES Y OERACIONES

### 11.1 Política de uso de correo electrónico

- La oficina de gestión de la información debe generar y adoptar un procedimiento para la administración de cuenta de correo electrónico.
- La oficina de gestión de la información asignará el nombre de usuario y contraseña.
- La contraseña asignada es genérica, el usuario está en la obligación de cambiarla inmediatamente. La contraseña deberá poseer un mínimo de 6 caracteres y deberá ser combinada con números y letras.
- Es responsabilidad de la oficina de gestión de la información, desbloquear las cuentas de usuarios que por una causa u otra hayan sido bloqueadas.
- Es deber de cada usuario asegurarse de cerrar la sesión de trabajo una vez finalice la utilización de todos los servicios a fin de que nadie más pueda utilizar su identificación.
- El uso del correo electrónico es única y exclusivamente para temas laborales según los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.
- Cada persona es responsable tanto del contenido del mensaje enviado, como de cualquier otra información adjunta en el mismo. Cada uno de los usuarios del servicio tiene la responsabilidad de asegurar el cumplimiento de las leyes de copyright y licenciamiento cuando se envían o reenvían correos electrónicos y archivos adjuntos. El no cumplimiento de lo estipulado anteriormente expone a la institución a demandas judiciales. Cualquier violación que se registre hará susceptible al infractor de medidas disciplinarias que podrán concluir en el máximo nivel de procesamiento permitido por la ley.
- La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas por la E.S.E Hospital Regional de Duitama.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la E.S.E Hospital Regional de Duitama y cada usuario, como responsable de su buzón debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto, la E.S.E. Hospital Regional de Duitama no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.
- Se prohíbe él envió cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

### 11.1 Política de uso de internet

- La oficina de gestión de la información es la responsable de implementar medidas lógicas y físicas que impidan el acceso indebido a internet por parte de los usuarios, esto será gestionado a través del Firewall de la entidad el cual deberá irse actualizando en temas de software y hardware para cubrir las necesidades de la institución.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, o que atente contra las leyes vigentes o políticas aquí establecidas.
- No está permitido el acceso y el uso de servicios interactivos o mensajería instantánea que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias de la E.S.E Hospital Regional de Duitama.
- No esta permitido el intercambio de información de propiedad o en custodia de la E.S.E Hospital Regional de Duitama salvo lo consagrado en la resolución 087 de 17 de abril de 2020 Política de tratamiento y protección de datos personales de le entidad.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

### 11.3 Política de control de cambios

- Todo cambio que se realice sobre la infraestructura tecnológica para el procesamiento de la información, comunicaciones y seguridad electrónica debe ser controlado, gestionado y autorizado adecuadamente, y debe ser sometido a una evaluación que permita identificar los riesgos, que pueden afectar la operación del negocio de acuerdo con los lineamientos establecidos.
- Los cambios estructurales que se planteen realizar sobre las plataformas críticas deben ser revisados por el Comité de Seguridad de la Información, el cual debe establecer los requerimientos de seguridad necesarios conforme a las políticas establecidas por la E.S.E Hospital San Rafael Tunja, que tengan como fin evitar un impacto adverso en las operaciones del negocio.
- La Gestión de Cambios debe contener como mínimo la identificación, justificación y evidencia de los cambios que se vayan a realizar sobre la infraestructura tecnológica, el alcance, autorización, el plan de trabajo para la definición de pruebas funcionales, responsabilidades definidas, la evaluación apropiada sobre el impacto potencial que estos pueden generar, un plan alternativo para abortar cambios no satisfactorios

(Rollback), eventos imprevistos y cualquier otro aspecto que se considere importante por los responsables del cambio.

### 11.4 Segregación de funciones

- Toda tarea en la cual el personal tengan acceso a la infraestructura tecnológica y a los sistemas de información debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la Institución.
- Todos los sistemas de disponibilidad crítica o media de la Institución, en lo posible, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

### 11.5 separación de ambientes

La E.S.E Hospital Regional de Duiatama ha definido diferentes ambientes para la ejecución de actividades de desarrollo, pruebas y puesta en producción de sus aplicaciones de negocio, con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes, los cuales son definidos de la siguiente manera:

- **Ambiente de Desarrollo:** Conjunto de elementos de hardware y software como compiladores, editores, instaladores de lenguajes de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones, entre otros.
- **Ambiente de Pruebas:** Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos para realizar los ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción de la E.S.E. Hospital Regional de Duitama.
- **Ambiente de Producción:** Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones de la E.S.E. Hospital Regional de duitama. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, base de datos, programas ejecutables o compilados.

## 12 ADMINISTRACION DE RECURSOS TECNOLOGICOS

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la E.S.E. Hospital Regional de Duitama es responsabilidad de la oficina de gestión de la información, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por la E.S.E. Hospital Regional de Duitama a través de esta área.
- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros.
- En el caso de personal, contratistas y/o terceros que requieran acceso a internet mediante la red inalámbrica Wi-Fi serán conectados por la oficina de gestión de la información asignando usuario en el servidor DHCP y los permisos correspondientes a través del firewall, de requerir permisos para accesos especiales estos deberán ser tramitados por el respectivo líder de proceso al cual se encuentra asignado el usuario.

## REFERENCIAS BIBLIOGRAFICAS


- Procedimientos De Seguridad de La Información https://www.mintic.gov.co/gestionti/615/articles5482_G3_Procedimiento_de_Seguridad.pdf
- Guía para la Gestión y Clasificación de Activos de Información http://www.mintic.gov.co/gestionti/615/articles5482_G5_Gestion_Clasificacion.pdf
- Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información http://www.mintic.gov.co/gestionti/615/articles5482_G14_Plan_comunicacion_sensibilizacion.pdf
- Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. http://www.mintic.gov.co/gestionti/615/articles 5482_G21_Gestion_Incidentes.pdf
- Modelo de Seguridad y Privacidad de la Información http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
- Código Penal Colombiano Ley 599 de 2000 - EVA - Función Pública (funcionpublica.gov.co)
- Código de Policía Código Nacional de Policía y Convivencia Ley 1801 de 2016 - Legislación colombiana 2020 (leyes.co)