E.S.E. HOSPITAL
San Rafael
DE ITAGÜÍ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

1. JUSTIFICACIÓN

La tecnología ha tenido un sin número de avances en estos últimos años y la forma de conectarnos ha aumentado, además, las aplicaciones y el software son cada vez más amigables y accesibles, pero esa facilidad de conexión también representa un aumento en los riesgos y estos hacen que la información y los recursos de una organización puedan llegar a ser vulnerados.

Por esta razón se hace necesario que la E.S.E Hospital San Rafael de Itagüí cuente con unas medidas de seguridad para proteger la información y los activos de la institución.

En este sentido, seguridad significa disponer de medios que permitan reducir lo más que se pueda, la vulnerabilidad de la información y de los recursos; logrando reducir el porcentaje de posibles riegos a un valor mínimo.

2. OBJETIVO GENERAL

Establecer las políticas que regulan la seguridad de la información en la E.S.E Hospital San Rafael de Itagüí y presentar en forma clara y coherente los elementos que conforman esta política, bajo el liderazgo del Área de Tecnologías y Sistemas de Información.

3. OBJETIVOS ESPECÍFICOS

- Cumplimiento por parte de todos los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el Hospital de la política de seguridad de la información en la E.S.E Hospital San Rafael de Itagüí.
- Velar por la protección al derecho de la confidencialidad y seguridad de la información de los usuarios internos y externos garantizando la generación, transmisión, uso, almacenamiento, conservación y divulgación de la información generada.
- Creación de procedimientos institucionales en el uso de tecnología adecuada y manejo de la información, cumpliendo con los principios consagrados en la Ley.

4. RESPONSABLE(S) DEL PLAN

Este plan está bajo el liderazgo del Área de Tecnologías y Sistemas de Información.

5. DEFINICIONES

Contraseña: Es una clave que permite acceder a un lugar, ya sea en el mundo real o en el virtual. Las contraseñas se utilizan por varios motivos: para preservar la intimidad, para mantener un secreto, como una medida de seguridad o como una combinación de todo ello.

https://www.definicionabc.com/tecnologia/contrasena.php

Encriptar: Ocultar datos mediante una clave para que no puedan ser interpretados por los que no la tienen.

https://languages.oup.com/google-dictionary-es/

Backup: Duplicado de un archivo informático que se guarda en previsión de la pérdida o destrucción del original': «Sería conveniente que hiciera una copia de seguridad de estos archivos» (Bustos Multimedia [Esp. 1996]). Esta es la expresión que debe usarse en español en sustitución del anglicismo back-up o backup. Se dice también, especialmente en América, (copia de) resguardo o respaldo.

https://www.rae.es/dpd/copia%20de%20seguridad

WinSCP: es una aplicación de Software Libre. WinSCP es un cliente SFTP gráfico para Windows que emplea SSH. También se puede seguir usando la versión anterior del protocolo. Su función principal es facilitar la transferencia segura de archivos entre dos sistemas informáticos, el local y uno remoto que ofrezca servicios SSH.

https://winscp.net/eng/docs/lang:es

6. META

Lograr implementar en un 90% el presente año una correcta política de seguridad de la información en la E.S.E Hospital San Rafael de Itagüí antes del 30 de noviembre del 2022, bajo los lineamientos del decreto 612 de 2018.

7. DESARROLLO DEL PLAN

La E.S.E. Hospital San Rafael de Itagüí consciente que la información es un activo valioso, definirá mecanismos que fortalezcan la capacidad del sistema para evitar las amenazas

latentes en el entorno, los accesos no autorizados, la manipulación o deterioro la información almacenada en él y fomentar el adecuado manejo de la información generada en los procesos Institucionales.

El Hospital se compromete a establecer las acciones para hacer cumplir la Ley y los reglamentos que, para el manejo de la información administrativa y técnica del Usuario, estén vigentes:

- ✓ **Confidencialidad:** Los Clientes Internos de la Institución deberán mantener la reserva sobre los documentos de trabajo que estén a su cargo o que manipulen para efectos de la prestación del servicio encomendado. Por lo tanto, deberán custodiar la información, evitando usos no autorizados. Toda la información debe ser guardada en carpeta única con rutas definidas y solamente la manipulará el personal autorizado por el Hospital.

- ✓ **Seguridad:** El Hospital no permitirá obtener información clínica o administrativa a personas diferentes al Usuario o que no hayan sido autorizados por el mismo para tal efecto. Para ello, el Hospital establecerá los procesos, asignará personal responsable y destinará un lugar adecuado para el cuidado y la protección de dicha documentación, así como la disponibilidad y el acceso oportuno por parte del Cliente Externo a este tipo de información.

- ✓ **Privacidad:** los usuarios deberán firmar un acuerdo de confidencialidad en caso de que terceras personas, ajenas a la empresa, deban acceder a la base de datos.

Seguimiento

Para garantizar el cumplimiento de la política de seguridad del sistema de información, desde el área de sistemas se toman las siguientes medidas:

- Capacitar a los usuarios del sistema de la E.S.E Hospital San Rafael de Itagüí en la Política de seguridad de la información.
- Informar a los usuarios del sistema en caso de modificaciones a la Política de seguridad de la información.
- Actualizar, vigilar y reportar posibles daños y cambios de los diferentes softwares que posee la institución a fin de aprovechar las mejoras realizadas a los programas, siempre y cuando se justifique esta actualización y se evite la proliferación de los virus en el sistema.
- Usar plataforma segura que cuente con un cortafuego (Firewall) para controlar el acceso desde Internet a la red.

- Definir los perfiles para acceder a los sistemas, estableciendo los permisos para grabar, modificar o consultar de acuerdo con el cargo de los clientes internos.

- Disponer de sitios adecuados para salvaguardar la información que se encuentre en diferentes medios (servidor NAS, papel, electrónico, magnético), asegurando las condiciones de almacenamiento adecuados y se generar informes trimestrales reportando el correcto uso de estos servicios.
- Que las áreas destinadas para la custodia de la documentación en la nube cumplan con las condiciones ambientales adecuadas, que incluyen manejo de temperatura, humedad relativa, ventilación e iluminación.
- Que los documentos físicos de imagen análoga, digital, CDS, cuenten con sistemas de almacenamiento especiales, como gabinetes, armarios, estanterías y bolsas plásticas de polipropileno.
- Que las diferentes áreas del hospital cuenten con suministros de seguridad, como extintores para casos de incendios, reguladores de corriente para caso de fallas eléctricas, entre otros y así para disminuir el riesgo de pérdida o daño de información por alteraciones en el suministro de energía eléctrica.
- Asegurar el respaldo de la información.
- Todos los clientes internos que deban tener acceso a las herramientas que apoyan el sistema de información, contaran con clave de acceso y perfiles de usuarios definidos que aseguren la autorización para grabar, modificar y consultar información.
- La divulgación de información generada en la E.S.E. Hospital San Rafael de Itagüi está bajo estudio, supervisión y aprobación por parte del área de sistemas y alta gerencia.

Normatividad de contraseñas

El objetivo de la presente norma es regular la creación y uso de contraseñas robustas, cuando este sea el mecanismo de autenticación usado para el acceso a determinados sistemas o servicios de la E.S.E. Hospital San Rafael de Itagüi.

Este documento se considera de uso interno de la E.S.E. Hospital San Rafael de Itagüi y por tanto no podrá ser divulgado salvo autorización de la Gerencia del Hospital.

La presente Normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el DECRETO NÚMERO 1317 DE 2013, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

Ámbito de aplicación

Esta Norma se aplica a todo el ámbito de trabajo de la E.S.E. Hospital San Rafael de Itagüi, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información del Área de sistemas.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la E.S.E. Hospital San Rafael de Itagüi, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de la E.S.E. Hospital San Rafael de Itagüi y utilicen contraseñas como medio de autenticación personal.

7.1 DESCRIPCIÓN

Normatividad:

Se tendrá un correcto uso para la generación de contraseñas bajo las siguientes directivas:

- La utilización de las claves para acceder al sistema de información está bajo la responsabilidad de cada usuario.
- Como norma general, las contraseñas deben ser fáciles de recordar y de introducir, aunque difíciles de adivinar y de descubrir por fuerza bruta (prueba exhaustiva de todas las posibilidades).
- Las contraseñas no deberán estar compuestas de datos propios que otra persona pueda adivinar u obtener fácilmente (nombre, apellidos, fecha de nacimiento, número de teléfono, números consecutivos, etc.).
- Las claves asignadas para acceder a los sistemas de información son de uso personal e intransferible.
- Los clientes internos deben cambiar la clave como mínimo **tres** veces al año o cuando se sospeche de alguna violación.
- Al dejar el puesto de trabajo, aunque sea por un momento, se deben dejar el equipo en modo se suspensión.
- Todo el personal activo y que cuente con usuario de red, que se desvincule de la institución y que tenga acceso al sistema de cómputo debe presentarse a la oficina de Sistemas para deshabilitar todas las claves de acceso asignadas.
- Una vez deshabilitadas las claves, el personal de Sistemas procede a diligenciar el formato Paz y salvo por retiro de un servidor público.

- Los privilegios de acceso a los equipos de cómputo y las redes deben cambiarse dos veces al año y serán asignados por el área de sistemas.
- Si el manejo de algunos archivos o equipos de cómputo requieren una clave o contraseña especial, esta debe ser notificada al área de sistemas.
- Las **contraseñas** deben tener una longitud mínima de 9 caracteres, que cuenten al menos con una letra mayúscula, un carácter especial y números no consecutivos.
- No utilizar la misma contraseña para distintos servicios web o en el acceso a distintos dispositivos.
- No debe permitirse apuntar las contraseñas en papel o bajo otro procedimiento o contenedor no seguro.

Sistema de verificación de contraseñas:

- El sistema de verificación no debe ofrecer al usuario mecanismos para recordar su contraseña, (tales como: "¿Cómo se llamaba tu primera mascota?", etc.).
- El sistema de verificación de contraseñas debería comparar la nueva contraseña del usuario con una "lista negra" de contraseñas inaceptables, por ser ampliamente usadas, deducibles o haber estado comprometidas, entre ellas: uso de caracteres repetitivos ("12345678") o secuenciales ("1234abcd"), palabras relacionadas con el contexto, tales como el nombre del organismo, del servicio y cualquiera de sus derivados. En estos casos, el sistema de verificación debería rechazar la contraseña e instar al usuario al generar una nueva contraseña.

- El sistema de verificación de contraseñas deberá limitar el número de intentos de acceso sin éxito.
- Aunque por defecto se oculte, el sistema debe permitir al usuario ver el contenido de su contraseña, dándole la oportunidad de visualizar los caracteres si considera que está en un entorno confiable.
- El sistema de verificación de contraseñas debe usar algoritmos de cifrado autorizados, así como un canal protegido cuando requiera una contraseña del usuario.
- El sistema de verificación debe memorizar las contraseñas de los usuarios utilizando procedimientos seguros, de forma que las haga resistentes a ataques offline.
- Todas las contraseñas del sistema serán analizadas por un programa de descifrado de contraseñas trimestralmente, anulándose las contraseñas que no superen dicha prueba.

Guía de backup copias de seguridad de la información

Las copias de seguridad son de gran importancia porque el activo más importante es la información, hoy en día todo depende de la información almacenada en el servidor, pero si por alguna razón como desastre natural o incendio, inundación falla de la computadora, entre otros, hay pérdida de esta información y es virtualmente imposible recuperarla sin copias de seguridad.

Todos los colaboradores de la E.S.E. Hospital San Rafael de Itagüi tienen sus datos almacenados en nuestros archivos compartidos y es el resultado de mucho esfuerzo y trabajo que ha realizado durante un largo período de tiempo, es por eso por lo que un pequeño fallo siempre inesperado puede acabar con años de trabajo en un instante.

Esta guía intenta explicar por qué hacer copias de seguridad es una operación necesaria y muy útil y también muestra cómo crear una copia de seguridad de la información.

Objetivo

Poder crear una guía de copias de seguridad y contar con un medio adecuado para proteger la información y definir la manera para proteger la información, restauración y correcto tratamiento en el evento de presentarse una pérdida de está.

Alcance

El alcance de esta guía inicia con la determinación de las copias de seguridad a realizar, que son carpetas que se han indicado con anterioridad a las cuales es necesario elaborar una copia de seguridad y que se encuentran ubicadas en los servidores de la E.S.E. Hospital San Rafael de Itagüi, que tiene el agente de Backup **WINSCP** Instalado (Herramienta con que cuenta el Hospital para realizar backups); lo cual termina con el almacenamiento de las cintas, restauración y la recuperación de información por parte de la oficina de sistemas.

Generalidades

El área de Sistemas se encarga de definir los medios adecuados, para guardar la información que se encuentra almacenada en los servidores la E.S.E. Hospital San Rafael de Itagüi y de esta manera minimizar el riesgo de pérdida de información a causa de diversos factores. La acción de almacenar la información nunca está garantizada, ya que existen diferentes eventos a tener en cuenta a la hora de decidir la realización de copias de seguridad:

- Daños en dispositivos en los que se guardan datos o información.
- Borrado o eliminación accidental.

- Formateo de dispositivos.
- Fallas en el hardware de soporte.
- Alteraciones en el suministro de la energía.
- Sobre escritura de datos en archivos con el mismo nombre.

La generación de copias de Seguridad debe corresponder a información de carácter institucional, debe excluirse la información de carácter personal, así como archivos de música y videos. Es responsabilidad de cada colaborador del hospital depurar la información de las carpetas compartidas a las cuales se les genera el backup.

La E.S.E. Hospital San Rafael de Itagüi cuenta con un servicio de custodia, almacenamiento interno y externo donde se realizan las copias de seguridad, estas copias son guardadas en bóveda, la cual tiene las normas mínimas de seguridad:

- Controladores de acceso de personal
- Cámaras de vídeo
- Controladores de Temperatura y humedad
- Sistema de Control de Incendio
- Vigilancia Personalizada interna y externa las 24 horas del día
- Monitoreo durante las 24 horas del día

El cuarto técnico debe estar en un área climatizada para que se conserve la información a salvo de los siguientes factores:

- Fuego
- Humedad
- Robo
- Inundaciones
- Campos Magnéticos

Procedimiento

El procedimiento de copias de seguridad (Backups) se realizan de dos maneras: Full Backup (Semanal) o Backup Incremental (Diario).

Tareas Programadas: En cada servidor se han programado tareas automáticas que se ejecutan periódicamente.

Periodicidad de las Copias: De acuerdo a la naturaleza de los archivos almacenados en los directorios o repositorios propios de cada aplicación se realizará el respaldo de la información dos veces al mes en una copia total y se ejecutará una copia incremental.

Recomendaciones

- Es muy recomendable que no se guarden archivos con nombres muy largos, ya que es de gran importancia en el momento de realizar una copia de seguridad porque los archivos que tienen nombres muy largos ocasionan problemas.

- Otro punto importante es nombrar los archivos con nombres que nos permitan reconocer que contenido tiene un archivo dado. Esto se hace para limitar a leer el nombre del archivo, y con esto debería ser suficiente para decidir si se guarda o se elimina.

Las copias de seguridad de la información almacenada en los servidores del hospital contasen con la siguiente estructura:

- Los responsables del manejo de cada uno de los sistemas deben realizar copias de seguridad diarias de las actividades o transacciones realizadas en los discos duros de las maquinas asignadas por el departamento de sistemas e Informática.
- Estas copias se programan para ser de manera automática en servidor.
- Los tiempos para realizar las copias de seguridad serán distribuidos de la siguiente manera, los miércoles se realiza una copia y se genera un registro de fecha y hora la cual se almacena para genera reporte, este proceso será por cada servidor.

7.2 PROGRAMACIÓN DE ESTRATEGIAS Y ACTIVIDADES

ESTRATEGIAS	ACTIVIDADES	RESPONSABLES	PLAZOS	MEDIOS DE VERIFICACIÓN
CAPACITACIONES	Capacitación de uso y creación de contraseñas seguras para personal administrativo	Área de sistemas	Febrero 18	Formato de lista de asistencia
	Capacitación Fortinet para el área de sistemas	Fortinet s.a	Marzo 14	Formato de lista de asistencia

ESTRATEGIAS	ACTIVIDADES	RESPONSABLES	PLAZOS	MEDIOS DE VERIFICACIÓN
	Capacitación ciberseguridad para personal administrativo	Área de sistemas	Junio 13	Formato de lista de asistencia
REVISION DE POLITICA DE DOMINIO	Revisión y análisis de política de servidor de dominio del hospital	Área de sistemas	Abril 18-25	Circular en intranet
REVISION DE POLITICA DE CORREOS	Revisión y análisis de política de correos para migración	Área de sistemas	Febrero 1-15	Circular en intranet

8. PRESUPUESTO

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
CAPACITACIONES	3	$ 250.000	$ 750.000
		TOTAL	$ 750.000

9. EVALUACIÓN

INDICADOR	FÓRMULA	META	FRECUENCIA
Control de amenazas web en equipo de computo	Total = host con antivirus instalado/ cantidad de host	90%	Anual
Control de seguridad en dispositivos de usuario final	Total = host integrados al Fortinet / cantidad de host	90%	Anual
Control de ataques cibernéticos	Total = peticiones DoS / peticiones totales al servidor	80%	Semestral

10. DOCUMENTOS DE REFERENCIA

CÓDIGO	NOMBRE
DECRETO NÚMERO 1317 DE 2013	El presente **Decreto** tiene como objeto reglamentar parcialmente la **Ley** 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Artículo 2°. Tratamiento de datos en el ámbito personal o doméstico.
UNE - ISO/IEC 27002:2005	proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.
UNE - ISO/IEC 27001:2007	Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
ISO/IEC 9001:2000 Sistemas de gestión de la calidad.	La Norma ISO 9001 especifica los requisitos para un sistema de gestión de la calidad que puedan utilizarse para su aplicación interna por las organizaciones, para certificación o con fines contractuales. Se centra en la eficacia del sistema de gestión de la calidad para dar cumplimiento a los requisitos del cliente.1 ene 2005

11. CONTROL DE DIVULGACIÓN

PROCESO- SERVICIO/ÁREA	ESTRATEGIA DE DIVULGACIÓN
Gerencia, Asesores de Gerencia, Coordinadores, Lideres, jefes de Áreas.	Se realizará una presentación concisa de los principales componentes del PETI, partiendo del diagnóstico inicial, explicando claramente las estrategias y proyectos como resultado del trabajo de análisis realizado.
Funcionarios de la E.S.E Hospital San Rafael de Itagüí.	Su divulgación se realizará a través de la realización de presentaciones sobre el impacto del PETI en la organización. Haciendo uso de: • Página WEB • Correo electrónico Institucional • Intranet • Circulares Internas

12. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCIPCIÓN DEL CAMBIO	SOLICITANTE

2022-01-23	01	Creación de documentación	Samuel Guevara Mejía Líder Sistemas

13. ANEXOS

CÓDIGO	NOMBRE
NA	NA

Elaboró/actualizó:	Revisó:	Aprobó:
Samuel Guevara Mejía Líder Sistemas	Jony Snejder Rojas Chavarría Jefe Oficina Asesora Planeación y Calidad Luis Fernando Cadavid Tejada Jefe Oficina Asesora Jurídica	Diego León Muñoz Zapata Gerente
Firma:	Firma:	Firma:
Fecha: 2022-01-20	Fecha: 2022-01-22	Fecha: 2022-01-23