

E.S.E. HOSPITAL NUESTRA SEÑORA DEL CARMEN DE TABIO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

[Escriba el subtítulo del documento]

Tabla de contenido

1. OBJETIVO GENERAL: 3

2. ALCANCE 3

3. RESPONSABLES 3

4. DESCRIPCION DEL PLAN 3

4.1. ACCIONES 3

4.2. ESTRATEGIAS 3

4.3. CONDICIONES GENERALES 4

4.4. RESPONSABLES 4

5. PLAN DE ACTIVIDADES: 6

6. **INDICADORES**: 6

7. BIBLIOGRAFÍA: 7

8. CONTROL DE CAMBIOS: 8

9. REVISIÓN Y APROBACIÓN: 8

1. OBJETIVO GENERAL:

Establecer reglas, dar a conocer el mejor manejo de las herramientas, para así disminuir riesgos de pérdidas de información, daños en equipos, líneas de red congestionadas, información filtrada con fines mal intencionados.

2. ALCANCE

Los funcionarios estén debidamente enterados sobre el manejo de información, el buen uso de los recursos informáticos, que tengan presente los riesgos que acarrea no llevar en práctica el plan de políticas de privacidad informática.

3. RESPONSABLES

Los funcionarios deben comprometerse a conocer el plan de políticas de privacidad y buen manejo informático, como deber cumplirlas y respetarlas para el desarrollo de las actividades eficazmente.

4. DESCRIPCION DEL PLAN

El propósito que tiene el Hospital Nuestra Señora Del Carmen al establecer el plan de políticas de privacidad y buen manejo informático es definir las normas y lineamientos a través de este documento para que se proteja la información de cada funcionario, que no se ponga en riesgo el rendimiento de los funcionarios y por ende afecten nuestra entidad.

4.1. ACCIONES

El propósito que tiene el Hospital Nuestra Señora Del Carmen al establecer el plan de políticas de privacidad y buen manejo informático es definir las normas y lineamientos a través de este documento para que se proteja la información de cada funcionario, que no se ponga en riesgo el rendimiento de los funcionarios y por ende afecten nuestra entidad.

Cualquier funcionario que se encuentre realizando una actividad que valla en contra del plan de políticas de privacidad y buen manejo informático, se le realizara seguimiento, si persiste se tomara el debido procedimiento a seguir

4.2. ESTRATEGIAS

LOS FUNCIONARIOS Y LA SEGURIDAD INFORMÁTICA

La responsabilidad por la seguridad de la información no sólo corresponde al área de Sistemas, sino que es una obligación de cada funcionario.

4.3. CONDICIONES GENERALES

Los Subgerentes y Coordinadores de Grupos de Trabajo son los responsables de identificar y valorar su información; puesto que, son los propietarios de la información.

Todos los servidores públicos deben seguir los lineamientos enmarcados en este documento.

La seguridad de la información debe estar enmarcada con los siguientes principios:

CONFIDENCIALIDAD: Se garantiza que la información sea accesible sólo a aquellas personas que estén autorizadas para tener acceso a ella. INTEGRIDAD: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

DISPONIBILIDAD: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

AUTENTICIDAD: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

AUDITABILIDAD: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

PROTECCIÓN A LA DUPLICACIÓN: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

LEGALIDAD: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

CONFIABILIDAD DE LA INFORMACIÓN: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

4.4. RESPONSABLES

1-Los mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento. De acuerdo con lo anterior, los usuarios no deben obtener las claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.

2-Los funcionarios son responsables de todas las actividades llevadas a cabo con su código de usuario y clave personal.

3-Los funcionarios deben informar inmediatamente al área que corresponda dentro del hospital toda vulnerabilidad encontrada en el sistema, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.

4-Los funcionarios no deben intentar sobrepasar los controles del sistema, examinar los computadores y redes del hospital en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento del sistema.

5-Los funcionarios no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas. Esto incluye los controles del sistema de información y su respectiva implementación.

6-Los funcionarios no deben destruir, copiar o distribuir los archivos del hospital sin los permisos respectivos.

7-Todo funcionario que utilice los recursos de sistema tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje.

8-Los computadores, sistemas y otros equipos deben usarse sólo para las actividades propias de la entidad, por lo tanto los usuarios no deben usar sus equipos para asuntos personales a menos que exista una autorización respectiva que avalúe el riesgo informático de tal labor.

9-Los funcionarios no deben tener ninguna red social, y si es necesaria se deberá pedir un permiso especial justificando la necesidad de la misma, igualmente para youtube.

10-Los funcionarios no deben instalar software en sus computadores sin las debidas autorizaciones.

11- Los funcionarios no deben ingerir alimentos en el área de trabajo debido a que corre riesgos el equipo de derrame de alimentos.

12-Los funcionarios no pueden trasladar los equipos de cómputo ni sus partes sin informar al área de sistemas.

13- Si los funcionarios necesitan un implemento ubicado en el área de sistemas deben realizar un formato solicitando el mismo, con un día de anticipación.

14- los funcionarios son responsables del estado de los equipos después del mantenimiento ya aplicado

15- si un equipo presenta fallas se debe inmediatamente informar al área de sistemas y evitar

16- Si tiene problemas con los equipos, la hora máxima de atención al caso es 1 hora, si después de una hora no se le da atención al caso, puede poner una queja directa.

17- Los funcionarios pueden manejar su información en la intranet (bdserver).

Por seguridad de la información y menos riesgo de pérdida de información.

18- El Funcionario debe manejar la mayor parte de información en la ubicación “disco c:” para disminuir la posibilidad de pérdida de información, y el robo de datos

5. PLAN DE ACTIVIDADES:

E.S.E HOSPITAL NUESTRA SEÑORA DEL CARMEN DE TABIO

ÍTEM	ACTIVIDADES		VIGENCIA 2022												TOTAL EJECUTADO	TOTAL PROGRAMADO	PENDIENTE POR EJECUTAR	PORCENTAJE DE EJECUCIÓN
			ENE	FEB	MAR	ABRI	MAY	JUN	JULIO	AGOSTO	EPTIEMBR	OCTUBRE	OVIEMBR	ICIEMBRE				
	PUBLICAR EN PAGINA WEB LA POLITICA DE SEGURIDAD	E													0	2	2	0%
		P																
		%																
	MANTENER AL TANTO LOS COLABORADORES SOBRE LA POLITICA	E													0	1	1	0%
		P																
		%																
	TENER EL CONTROL DE TODOS LOS CORREOS ELECTRONICOS DE LA INSTITUCION	E													0	2	2	0%
		P																
		%																
	MANTENER SALVAGUARDADA LAS BASES DE DATOS BDSEVER	E													0	2	2	0%
		P																
		%																
	MANTENER SALVAGUARDADA LA INFORMACION BDSERVER	E													0	2	2	0%
		P																
		%																
	VELAR POR LA CONFIDENCIALIDAD DE LA INFORMACION	E													0	2	2	0%
		P																
		%																
	MANTENER EL FIREWALL ACTIVO, DEFENDER	E													0	2	2	0%
		P																
		%																
	TENER LICENCIADO Y ACTUALIZADO EL ANTIVIRUS (ESET NOT32)	E													0	1	1	0%
		P																
		%																

6. **INDICADORES**:

PUBLICAR EN PAGINA WEB LA POLITICA DE SEGURIDAD
MANTENER AL TANTO LOS COLABORADORES SOBRE LA POLITICA
TENER EL CONTROL DE TODOS LOS CORREOS ELECTRONICOS DE LA INSTITUCION
MANTENER SALVAGUARDADA LAS BASES DE DATOS BDSEVER
MANTENER SALVAGUARDADA LA INFORMACION BDSERVER
VELAR POR LA CONFIDENCIALIDAD DE LA INFORMACION
MANTENER EL FIREWALL ACTIVO, DEFENDER
TENER LICENCIADO Y ACTUALIZADO EL ANTIVIRUS (ESET NOT32)

7. BIBLIOGRAFÍA:

ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la Gestión de la Seguridad de la Información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información. En el siguiente esquema se pretende abordar los principales contenidos de la norma.

ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

Ley Estatutaria 15 81 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.

Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

8. CONTROL DE CAMBIOS:

Tabla. Control de Cambios en este Documento

FECHA	VERSIÓN	No. SOLICITUD DE ACTUALIZACIÓN	CAMBIO REALIZADO	RESPONSABLE
2021-01-15	01	Creación	Creación	Líder de Sistemas
2022-01-14	02	Actualización	Actualización y ajuste de contenido	Líder de Sistemas
2023-01-20	03	Actualización	Actualización y ajuste de contenido	Líder de sistemas
2024-01-22	04	Actualización	Actualización y ajuste de contenido	Líder de Sistemas

9. REVISIÓN Y APROBACIÓN:

Nombre	Fabián Pulido	Jenny Pilar Gómez Plazas	Isabel Rocio Garzón Forero
Cargo	Líder de Sistemas	Asesora de Planeación	Gerente
	Elaboró	Revisó	Aprobó