

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GC-SO-FO-07
		VERSIÓN: 01
	POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	FECHA: 21/09/2020
		TRD:
		PÁGINA: 1 de 5

RESOLUCION No. 0313-2022
(09 noviembre de 2022)

POR MEDIO DE LA CUAL SE ESTABLECE LA POLITICA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL ESE

El Gerente del Hospital Departamental San Rafael De Zarzal E.S.E., Valle del Cauca, en uso de las atribuciones legales y constitucionales, y demás normas concordantes y reglamentarias, y,

CONSIDERANDO

La Norma ISO 27001: Norma internacional de Seguridad de la Información que pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la trata.

El Dominio A16 ISO 27001. Para la gestión de incidentes de la seguridad de la información. “Los incidentes en la seguridad de la información parecen inevitables hoy en día por lo que no tenemos más remedio que plantearlos como vamos a gestionar dichos incidentes de la manera más ágil y eficiente para la organización”.

El Manual de seguridad y privacidad de la información (Min TIC), Estrategia de Gobierno Digital.

El Numeral 8.2 Fase de planificación - Políticas de Seguridad y Privacidad de la Información

El Manual del Sistema Integrado de Gestión – MEN. Sistema de Gestión de Seguridad de la Información

RESUELVE:

CAPITULO I
DISPOSICIONES GENERALES

ARTICULO 1. OBJETO. Gestionar adecuadamente todos los incidentes de seguridad de la información dando cumplimiento a los procedimientos establecidos.

ARTICULO 2. AMBITO DE APLICACIÓN. Esta política aplica para todos los usuarios y proveedores que detecten un evento o incidente de seguridad de la información el cual deben reportar, adecuadamente, de acuerdo con los procedimientos establecidos.

ARTICULO 3. DEFINICIONES.

- a) **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- b) **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- c) **Confidencialidad:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.
- d) **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GC-SO-FO-07
		VERSIÓN: 01
	POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	FECHA: 21/09/2020
		TRD: PÁGINA: 2 de 5

- e) **Dato:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- f) **Activo de Información:** Es todo aquello que en el Ministerio de Educación Nacional es considerado importante o de alto valor para la entidad, porque contiene información importante, como son los datos creados o utilizados por procesos de la organización, en medio digital, en papel o en otros medios. Ejemplos: bases de datos con usuarios, contraseñas, números de cuentas, informes etc.
- g) **Evento de seguridad de la información:** Ocurrencia identificada de una condición de un proceso, sistema, servicio, red o del entorno que indica una posible violación de las políticas de seguridad de la información del Ministerio de Educación Nacional, o una falla en los controles o situación previamente desconocida que puede ser relevante para la seguridad de la información.
- h) **Incidente de seguridad de la información:** Uno o más eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la entidad y amenazan la confidencialidad, integridad y/o disponibilidad de la información del Ministerio de Educación Nacional.
- i) **SGSI:** Sistema de Gestión de Seguridad de la Información.
- j) **Seguridad digital:** Es el área de la informática que se enfoca en la protección de la infraestructura computacional, todo lo relacionado con esta y, especialmente, en la información contenida o circulante. Incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

ARTICULO 4. Directrices.

Gestión de incidentes y mejoras de la seguridad de la información

Responsabilidades y procedimientos

2

CONTROL	DIRECTRICES	ACTORES	SOPORTE /FORMA DE COMUNICAR DIRECTRICES
Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	digital dentro del área de sistemas de información	Área de Sistemas de Información	Roles y responsabilidades
	Definir el procedimiento de atención de incidentes de seguridad de la información del área de sistemas de información.		Procedimiento gestión de incidentes
	Dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados en el área de sistemas de información.		Procedimiento Gestión de Incidentes
	Realizar sensibilización a todos los colaboradores y terceros sobre incidentes de seguridad de la información.		reporte del incidentes Incidentes de seguridad de la Información al medio de comunicaciones Actividades de sensibilización

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GC-SO-FO-07 VERSIÓN: 01
	POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	FECHA: 21/09/2020 TRD: PÁGINA: 3 de 5

Reporte de eventos de seguridad de la información

CONTOL	DIRECTRICES	ACTORES	SOPORTE /FORMA DE COMUNICAR DIRECTRICES
Informar sobre los eventos de seguridad de la información a través de los canales de gestión apropiados,	Reportar de forma inmediata de acuerdo con el procedimiento previsto los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.	Todos los colaboradores y terceros del Hospital	Reporte por correo electrónico o medio de comunicaciones interno sobre los incidentes

Evaluación de eventos de seguridad de la información y decisiones sobre ellos

CONTROL	DIRECTRICES	ACTORES	SOPORTE /FORMA DE COMUNICAR DIRECTRICES
Evaluar los eventos de seguridad de la información y decidir si se van a clasificar	Evaluar cada evento o incidente de seguridad de la información usando la escala de clasificación de eventos e incidentes de seguridad de la información con el fin de poder determinar clasificación y priorización. De acuerdo con el definido en el procedimiento previsto.	Área de Sistemas de Información	Reporte por correo electrónico o medio de comunicaciones interno sobre los incidentes

CONTROL	DIRECTRICES	ACTORES	SOPORTE /FORMA DE COMUNICAR DIRECTRICES
Evaluar los eventos de seguridad de la información y decidir si se van a clasificar	Informar los resultados para referencia y verificación futuras.	Área de Sistemas de Información	Informar al comité de Seguridad de la Información

Respuesta a incidentes de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE /FORMA DE COMUNICAR DIRECTRICES
Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos que serán informados en el canal de comunicaciones del Hospital	Responder a los incidentes de seguridad de la información que se presenten en el Hospital Departamental San Rafael de Zarzal E.S.E. La respuesta debe incluir lo siguiente: <ul style="list-style-type: none"> ✓ Recolectar evidencia lo más pronto posible después de que ocurra el incidente. ✓ Llevar a cabo análisis forense de seguridad de la información, según se requiera. ✓ Llevar el asunto a una instancia superior, según se requiera. ✓ Asegurarse de que todas las actividades de respuesta involucradas se informen adecuadamente para análisis posterior. ✓ Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo. ✓ Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente. 	Área de Sistemas de Información	Informar de Gestión de Incidentes de Seguridad de la Información Planes de mitigación de vulnerabilidades Ejecutados

Calle 5 No. 6-32 Zarzal - Valle del Cauca Tel. 222 0046 - 222 0043 - 2209914 Fax. Ext 104 y 106 Urgencias 222 1011

NIT: 891900441-1 - www.hospitalsanrafaelzarzal.gov.co

Gerencia@hospitalsanrafaelzarzal.gov.co - Hospitaldepartamentalsanrafael@hotmail.com

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	CÓDIGO: DE-PL-CI-01
		VERSIÓN: 01
	RESOLUCION	FECHA: 21/09/2020
		TRD:
		PÁGINA: 4 de 5

CONTROL	DIRECTRICES	ACTORES	SOPORTE /FORMA DE COMUNICAR DIRECTRICES
	<p>✓ Una vez que el incidente se haya tratado lo suficiente, informar que el incidente culmino.</p>	Área de Sistemas de Información	Reportar Incidentes de seguridad de la información
	<p>Escalar los incidentes a niveles superiores o control interno en caso de que sea requerido.</p>		Registro comunicación

Aprendizaje obtenido de los incidentes de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE /FORMA DE COMUNICAR DIRECTRICES
Usar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la posibilidad o el impacto de incidentes futuros	Informar todos los incidentes de seguridad de la información que pasen en el Hospital al comité de seguridad de la información y a todos los usuarios del Sistema.	Área de Sistemas de Información	Gestión de seguridad de la información
	Llevar un Registro de los incidentes de seguridad de la información reportados y atendidos en el Hospital Por medio del aplicativo dispuesto para tal fin.		Gestión de Incidentes de seguridad de la información

Recolección de evidencia

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Desarrollar y seguir procedimientos internos cuando se trata con evidencia para propósitos de acciones legales y disciplinarias en el Hospital Departamental San Rafael de Zarzal E.S.E.	Área de Sistemas de Información	Procedimientos Documentación aplicable
	<p>Los procedimientos para evidencia deben contener actividades tales como; identificación, recolección, adquisición y preservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos, por ejemplo, encendidos o apagados. Los procedimientos deben tener en cuenta:</p> <p>La cadena de custodia; La seguridad de la evidencia; La seguridad del personal; Los roles y responsabilidades del personal involucrado; La competencia del personal; La documentación; Las sesiones informativas. Para el transporte de elementos, se debe llevar la cadena de custodia.</p>		Procedimientos y Documentación aplicable

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA NIT: 891900441-1	CÓDIGO: DE-PL-CI-01
		VERSIÓN: 01
	RESOLUCION	FECHA: 21/09/2020
		TRD: PÁGINA: 5 de 5

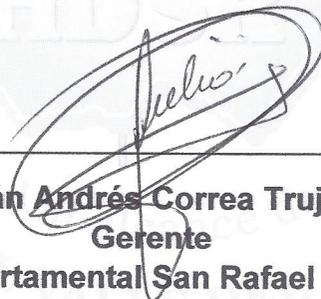
ARTICULO 5. INFORMACIÓN DE CONTACTO. Cualquier inquietud relacionada con la guía política de gestión de incidentes de seguridad de la información, favor remitirla al correo sistemas@hospitalsanrafaelzarzal.gov.co

ARTICULO 6. REVISIÓN DE LA GUÍA. Esta política debe ser revisada por el comité de seguridad de la información mínimo una vez al año.

ARTICULO 7: La presente resolución rige a partir de la fecha de su expedición

COMUNIQUESE, NOTIFIQUESE Y CUMPLASE:

Dada en Zarzal Valle del Cauca, a los nueve (09) días del mes de noviembre del dos mil veintidos (2022).



Julián Andrés Correa Trujillo
Gerente
Hospital Departamental San Rafael Zarzal E.S.E.

Elaboro: Sandra Rincón – Coordinadora de sistemas
Reviso: Paulo Castillo Ferreira – Asesor de Calidad
Aprobó: Julián Andrés Correa Trujillo – Gerente