RESOLUCION No. 351

Fecha: 23 JUL 2020

"Por medio de la cual se adopta la política de Seguridad y Privacidad de la Información de la ESE CARMEN EMILIA OSPINA," con el fin de dar cumplimiento a las actividades desarrolladas en la implementación del Modelo de Seguridad y Privacidad de la Información que se encuentra realizando la ESE CARMEN EMIILIA OSPINA, se elaboran una serie de políticas específicas que se describen a continuación:

POLITICAS DE SEGURIDAD DE LA INFORMACION – ESE CARMEN EMILIA OSPINA

1. Introducción

La ESE CARMEN EMILIA OSPINA, Garantiza la gestión de la información, está comprometida con la implementación del sistema de gestión de seguridad de la información, buscando establecer un marco de confianza para el ejercicio de sus deberes con el Estado y los ciudadanos, con base en el estricto cumplimiento de la normatividad.

Esta Política debe ser adoptada por los funcionarios, contratistas, proveedores, ciudadanía y usuarios, que tengan algún tipo de relación con la ESE CARMEN EMILIA OSPINA. La Política está basada en el cumplimiento de la normatividad legal colombiana vigente, Decreto 1078 de 2015, que hace referencia al Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones.

2. Objetivo:

Establecer los lineamientos y directrices que permitan el control efectivo de la información en la ESE CARMEN EMILIA OSPINA, como herramienta que logre identificar y minimizar los riesgos a los cuales se expone la Información, garantizando la disponibilidad, integridad y confidencialidad de la información.

3. Compromisos De La Alta Dirección

La Gerencia de la ESE CARMEN EMILIA OSPINA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad y privacidad de la información (SGSI), buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

De igual manera garantiza la disposición de los recursos necesarios para que la entidad en términos de seguridad de la información pueda acoplar sus procesos al modelo MSPI.

4. Alcance

La presente política aplica a toda la Entidad, sus funcionarios, contratistas, terceros, Proveedores de la ESE CARMEN EMILIA OSPINA y la ciudadanía en general.

5. Responsabilidades De Funcionarios, Contratistas Y Terceros

Es responsabilidad de los funcionarios, contratistas y terceros salvaguardar la información institucional de la ESE CARMEN EMILIA OSPINA, garantizando así la confidencialidad, integridad y disponibilidad de la información teniendo como responsabilidades:

a. Cumplir las políticas de seguridad y privacidad de la información descrita en el presente documento.
b. Reportar los incidentes de seguridad de la información a la mayor brevedad mediante los canales establecidos para ello.
c. Utilizar los sistemas de información, el acceso a la red y la información únicamente para las funciones a su cargo y los propósitos establecidos en las políticas de seguridad de la información.
d. Incorporar la seguridad de información como parte de las actividades y tareas bajo su responsabilidad.
e. Utilizar únicamente software y demás recursos tecnológicos autorizados.

6. Definiciones:

Amenaza: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Copias de respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Dato: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

Disponibilidad: Acceso y uso de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Gestión de Riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la entidad. Incluye la valoración de riesgos y el tratamiento de los riesgos.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.

Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

MSPI: Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad: Una condición que resulta del establecimiento y mantenimiento de medidas de protección que permiten a una empresa cumplir su misión o funciones críticas a pesar de los riesgos que plantean las amenazas a su uso de los sistemas de información. Las medidas de protección pueden incluir una combinación de disuasión, evitación, prevención, detección, recuperación y corrección que debe formar parte del enfoque de gestión de riesgos de la empresa.

Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Tratamiento del riesgo: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

Usuario: Datos dotados de significado y propósito. Datos relacionados que tienen significado para la Entidad.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que permite potencialmente que una amenaza afecte a un activo.

7. POLITICA GENERAL

La información que se maneja en la ESE CARMEN EMILIA OPSINA, solamente podrá ser utilizada con fines de interés público de conformidad con Los estatutos, constitución y las leyes.

La ESE CARMEN EMILIA OSPINA, cuenta de manera permanente y con Licencias y soporte de Sistemas Antivirus.

La ESE CARMEN EMILIA OSPINA, contrata de manera continua el servicio de FIREWALL, con políticas de navegación, VPN, Direcciones Publica y el monitoreo respectivo.

La ESE CARMEN EMILIA OSPINA, mantiene sus activos de información actualizados con la clasificación respectiva.

El área TIC de la ESE CARMEN EMILIA OSPINA, realiza las copias de seguridad de las aplicaciones, bases de datos y servicios, de acuerdo a lo establecido en los procedimientos del proceso.

El área TIC de la ESE CARMEN EMILIA OSPINA, publica en su INTRANET y sensibiliza a través de capacitaciones al personal en Tips y noticas referentes a seguridad y privacidad de la información.

Las herramientas y servicios informáticos asignados a cada usuario, son para uso limitado a la función institucional.

Todos los servidores públicos, contratistas y terceros que conforman las diferentes dependencias de la ESE CARMN EMILIA OSPINA, deberán clasificar la información que tengan bajo su custodia en alguna de las categorías establecidas.

La información confidencial de terceros que por cualquier circunstancia se conozca por parte de la ESE CARMEN EMILIA OSPINA, debe ser tratada bajo los mismos lineamientos establecidos para el tratamiento de la información.

La ESE CARMEN EMILIA OSPINA, avala el Teletrabajo, Para el acceso remoto a los servicios tecnológicos que provee la ESE CARMEN EMILIA OSPINA, se deberá hacer solicitud a La oficina TIC (o quien haga sus veces), por parte del jefe inmediato y/o supervisor de contrato de la persona quien vaya a hacer uso de la conexión. La conexión remota que habilite equipo de Sistemas de Información y Tecnología, (o quien haga sus veces) deberá ser temporal y garantizar la seguridad.

Toda la información catalogada por las áreas como critica debe contar con copias de respaldo para garantizar su seguridad.

Los centros de cómputo y procesamiento de información son áreas de acceso restringido por tal motivo el ingreso y permanencia debe ser controlado y supervisado.

El acceso a los diferentes equipos informáticos y sistemas de información debe hacerse a través de los mecanismos de autenticación establecidos de acuerdo con los niveles de seguridad.

El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la entidad está prohibido.

Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas:

a. Suministrar información confidencial o que tenga carácter reservado a quien no tenga derecho a conocerla.

b. Usar la información con el fin de obtener beneficio propio o de terceros.

c. Ocultar la información maliciosamente causando cualquier perjuicio.

d. Hacer pública la información sin la debida autorización.

e. Hurtar software de La ESE CARMEN EMILIA OSPINA (copia o reproducción entre usuarios finales).

f. Descargar software, a través de Internet sin la debida autorización.

g. Intentar modificar, reubicar o sustraer equipos de cómputo, software, Información o periféricos sin la debida autorización.

h. Capturar sin autorización la información de los accesos de otros usuarios a los sistemas.

I. Utilizar la infraestructura Tecnológica, de la ESE CARMEN EMILIA OSPINA (computadores, software, información o redes) para acceder a recursos externos con propósitos ilegales o no autorizados.

j. Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.

k. Lanzar cualquier tipo de virus, gusano o programa de computador cuya intención sea hostil o destructiva.

l. Descargar o publicar material ilegal, o implique la vulneración de derechos de terceros, o material nocivo.

m. Uso personal de cualquier recurso informático de la ESE CARMEN EMILIA OSPINA, para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material prohibido.

n. Acceder sin autorización a información o documentos públicos que tengan carácter reservado por disposición constitucional o legal.

o. Violar cualquier Ley o Regulación Nacional respecto al uso de sistemas de información.

8. Vigencia

La presente política rige a partir de su publicación y su vigencia estar supeditada a las modificaciones de normatividad Nacional y/o mejoraras al Modelo de Seguridad y Privacidad de la Información.

Dado en Neiva, a los 23 de Julio del 2020

Atentamente,

JOSE ANTONIO MUÑOZ PAZ
GERENTE.

Reviso: **CRHISTIAN YOHANNY RAMIREZ CARDOZO**
Asesor Jurídico

Elaboro: **JOSE YAMIL LAGUNA ROJAS**
Profesional Especializado I Área TIC