PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Biblioteca Virtual Calle 83 avenida Pedro Tafur Tel. (8) 2795992
E-mail: *imdrideportes@gmail.com* Pagina Wed: *www.imdri.gov.co*
Ibagué Tolima

Introducción

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Contraloría Municipal de Villavicencio (CMV) con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información

Objetivo

La entidad cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los riesgos existentes.

DOCUMENTACION REFERENCIA

ISO 27001:2013 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de seguridad de la información.
ISO 22301:2012 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de continuidad del negocio
LEY 1581:2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Borrador del manual para la implementación de la Política de Gobierno Digital

- ✓ Mantener sus estaciones de trabajo y servidores actualizados, es decir, el sistema operativo debe tener al día las actualizaciones críticas y de seguridad, así como tener políticas de seguridad (hardening), lo que minimiza los riesgos de seguridad. También se requiere que los sistemas operativos tengan un antivirus actualizado.

- ✓ Verificar el uso de buenas contraseñas para usuarios y servidores, es decir, se debe tener una buena práctica de generación de contraseñas y su custodia. Se recomiendan contraseñas alfanuméricas, mínimo 8 caracteres.

- ✓ Verificar la comunicación entre usuarios a través de estaciones de trabajo o servidores, con el fin de que se utilicen protocolos de seguridad de acuerdo

  Con el análisis de riesgos realizado, de manera que la comunicación no se haga vulnerable. Así los inicios de sesión están protegidos, que los certificados digitales sean válidos y los sitios web asegurados (https, ftps, entre otros.)

- ✓ Generar conciencia sobre los ataques vía phishing, suceden a través de correo generalmente, otras veces a través de redes sociales; con el objetivo de extraer información de la entidad, por ellos se debe recomendar no abrir enlaces de correo desconocido, ingresar a sitios de dudosa reputación, no compartir información en redes sociales con perfiles desconocidos o abrir enlaces a través de chats.

- ✓ Recomendar a los usuarios de la entidad no registrar datos personales en sitios web o redes sociales.

- ✓ Recomendar a los usuarios no descargar software, el cual puede tener contenido malicioso para afectar la seguridad de la entidad; tal como sucede con el software ilegal.

- ✓ Recomendar a los usuarios de la entidad realizar una copia de seguridad de la información que maneja, así como la entidad debe tener una política de respaldo sobre sus activos más importantes. Todo esto con el objetivo no

  Perder el control sobre la información en caso de un incidente de seguridad.

- ✓ Verificar la infraestructura de seguridad que posee la entidad, como son anti-DDOS, WAF, Firewall entre otros; con el objetivo de que estén actuando de la manera indicada y reportando eventos e incidentes a los administradores de dicha infraestructura.

- ✓ Verificar el código de los sitios web de la entidad, para evitar la ejecución de malware, minado de criptomonedas, revisar la versión del web Server para que no presenten vulnerabilidades de día cero (O), así como el gestor de contenido.

- ✓ Verificar la forma de realizar consultas a las bases de datos de la entidad, para evitar inyección a través de consultas mal formadas que permitan extraer información.

Actualizar el Manual de Políticas de Seguridad del Instituto