2

RESOLUCIÓN 20231044

"Por medio del cual se aprueba y adopta la versión No. 1 de la Política de Tratamiento Web Condiciones Mínimas Técnicas y de Seguridad Digital del Instituto para el Desarrollo de Antioquia-IDEA"

El Gerente General del Instituto para el Desarrollo de Antioquia – IDEA – en uso de sus facultades constitucionales y legales, y en especial las conferidas por el artículo 9 y ss. de la Ley 489 de 199, en la delegación del 19 de diciembre de 2023 de la Junta Directiva del IDEA en la sesión número 21; las conferidas en el numeral 4 y 21 del artículo Décimo sexto de la Resolución de Junta Directiva número 006 del 2014 (Estatutos del Instituto para el Desarrollo de Antioquia – IDEA-) y,

CONSIDERANDO:

1. Que conforme al principio de "masificación del gobierno en línea", hoy Gobierno Digital, consagrado en el numeral 3 del artículo 4o de la Ley 1341 de 2009, el Estado requiere promover el desarrollo de contenidos y aplicaciones, la prestación de servicios que usen Tecnologías de la Información y las Comunicaciones y la masificación del gobierno digital.
Que la Resolución 1519 de 2020 de MINTIC define los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

2. Que la Ley 1712 de 2014, en su artículo 3o, contempla el desarrollo del principio de la calidad de la información, y determina que la información pública debe ser procesable en formatos accesibles.

3. Que, con el objeto de dar cumplimiento a la ley, el Estado requiere definir los estándares de publicación y divulgación de la información pública, de forma que facilite el cumplimiento de las obligaciones a cargo de los sujetos, todo en garantía del derecho de acceso a la transparencia en la información pública, en concordancia con lo consagrado en el parágrafo 3 del artículo 9o de la Ley 1712 del 2014 y el artículo 2.1.1.2.1.1 del Decreto 1081 del 2015.

4. Que el día 19 de diciembre de 2023, se llevó a cabo la sesión ordinaria No. 21 de Junta Directiva del Instituto para el Desarrollo de Antioquia – IDEA donde se delegó al Gerente General para aprobar y adoptar la Política de Tratamiento Web Condiciones Mínimas Técnicas y de Seguridad Digital del Instituto de acuerdo con los lineamientos de MINTIC, con un plazo máximo hasta el 31 de enero de

2024.

En mérito de lo expuesto, el Gerente General del Instituto para el Desarrollo de Antioquia – IDEA,

RESUELVE:

PRIMERO: APROBAR Y ADOPTAR LA POLÍTICA DE TRATAMIENTO WEB CONDICIONES MÍNIMAS TÉCNICAS Y DE SEGURIDAD DIGITAL DEL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA-IDEA versión No. 1, la cual se anexa al presente acto administrativo y se entiende que hace parte integral del mismo.

SEGUNDO: IMPLEMENTACIÓN, DIFUSIÓN Y SENSIBILIZACIÓN. Ordenar la implementación y difusión a través de los medios institucionales y sensibilización de la Política de Protección de tratamiento web y de seguridad digital, aprobada y adoptada en el artículo anterior.

TERCERO. VIGENCIA. La presente Resolución rige a partir de su publicación y comunicación, de conformidad con lo dispuesto por el artículo 65 de la Ley 1437 de 2011, de manera especial, previa publicación y comunicación a los empleados del IDEA y demás interesados; y deroga todas las disposiciones que le sean contrarias.

CUARTO: PROCEDENCIA DE RECURSOS. Contra esta Resolución no procede recurso alguno, de conformidad con lo establecido con el artículo 75 de la Ley 1437 de 2011.

Dada en Medellín, a los **29-12-2023**

PUBLIQUESE, COMUNÍQUESE Y CÚMPLASE

JULIÁN SANTIAGO VÁSQUEZ ROLDÁN
Gerente General

Instituto para el Desarrollo de Antioquia -IDEA

Proyectó: SANDRA PATRICIA MENDOZA HINESTROZA
SECRETARIO
DIRECCION DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACION

Aprobó: ANA MARIA GOMEZ CARDONA
GERENTE
GERENCIA DE RIESGOS

Aprobó: ALEXANDER CLAVIJO RAMIREZ
DIRECTOR TÉCNICO
DIRECCION DE CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACION

Aprobó: JAIR ANTONIO VILLANUEVA RICARDO
GERENTE
GERENCIA DE TI Y OPERACIONES

Aprobó: ISABEL CRISTINA SALAZAR GIRALDO
JEFE DE OFICINA
OFICINA DE PLANEACION ESTRATEGICA

Aprobó: JUAN CARLOS LEDEZMA MATURANA
DIRECTOR TÉCNICO
DIRECCIÓN JURIDICA

Aprobó: LINA MARIA RAMIREZ MURIEL
SECRETARIO GENERAL DE ENTIDAD DESCENTRALIZADA
SECRETARÍA GENERAL

POLÍTICAS DE TRATAMIENTO WEB CONDICIONES MÍNIMAS TÉCNICAS Y DE SEGURIDAD DIGITAL

Tabla de contenido

1. OBJETIVO

Garantizar la seguridad digital y mitigar riesgos cibernéticos o filtración de datos personales o sensibles de la información administrada el INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA - IDEA -, en la página Web y los diversos canales digitales.

2. NORMATIVIDAD APLICABLE

- ✓ Constitución Política de Colombia
- ✓ Ley 1581 de 2012
- ✓ Decreto 1074 de 2015 Capitulo 25 y Capitulo 26 compilatorios de los decretos:
  - Decreto 1377 de 2013
  - Decreto 886 de 2014
- ✓ Resolución 1519 del 2020 de MINTIC

3. GLOSARIO

Establecidas en el artículo 3 de la Ley Estatutaria 1581 de 2012 y artículo 2.2.2.25.1.3 Capitulo 25 del Decreto compilatorio 1074 de 2015 (Artículo 3 del Decreto 1377 de 2013) y en la resolución 1519 del 2020 de MINTIC.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Cookie: Archivo creado por los sitios web en donde se almacenan datos sobre la navegación del usuario.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Debe entonces entenderse el “dato personal” como una información relacionada con una persona natural (persona individualmente considerada).

Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato Semiprivado: Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Dato Privado: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de

datos de los responsables de operadores que presten servicios de comunicación electrónica.

Dato Sensible: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

ColCERT: Grupo de Respuesta a Emergencias Cibernéticas del Ministerio de Defensa Nacional.

CSIRT – Gobierno: Grupo de Respuestas a Incidentes de Seguridad Informática del Gobierno Nacional.

Defacement: Denominación en inglés que hace referencia al tipo de ataque cibernético, bajo el cual se desconfiguran los contenidos del sitio o portal web, incluso poniéndoles “otra cara” mediante colores, imágenes o contenidos no originales.

Aseguramiento de variables en el código: Proceso de validación para confirmar que los datos ingresados en una variable correspondan con las entradas o caracteres válidos asignados por defecto en su configuración.

Hardening (endurecimiento): En el contexto de seguridad digital, implica eliminar todas las configuraciones por defecto, reduciendo las vulnerabilidades y asegurando los sistemas e infraestructuras digitales.

Plugins: Herramientas o aplicaciones de software que realizan funciones específicas, añadiendo a un software principal.

Políticas de origen de las cabeceras: Serie de reglas que garantizan la seguridad de las cabeceras del protocolo HTTP.

Script: Es un conjunto de comandos que ejecutan diversas funciones en los dispositivos electrónicos, entre dichas funciones están: interactuar con el sistema operativo y el usuario, combinar componentes, controlar programas y salidas de datos, configuraciones, entre otras. Su objetivo es agilizar y facilitar procesos administrativos y operacionales.

Token de CSRF: Código único de seguridad enviado en forma remota para validar la identidad del usuario.

4. DATOS DE NAVEGACIÓN

Al ingresar a los portales web del Instituto los datos mínimos recolectados son:

- Dirección IP Origen.
- URL por la que se ingresa, que puede estar redireccionando a la página del IDEA.
- Fecha y hora del ingreso.
- Otros parámetros relativos al tipo de conexión, navegador y sistema operativo del usuario.

Estos datos se utilizan con el propósito de obtener información estadística y poder proponer controles de ciberseguridad.

Cuando en el portal, se utiliza la opción de contacto, la persona puede elegir si desea proporcionar su información personal, como, por ejemplo, su nombre, dirección postal o electrónica, teléfono, entre otros, para que el Instituto pueda comunicarse y tramitar su solicitud o proporcionar información.

5. ATENCIÓN A LOS TITULARES DE DATOS

El Oficial de Protección de Datos de IDEA será el encargado de la atención de peticiones, consultas y reclamos por medio de los cuales el titular de los datos puede ejercer sus derechos. El Instituto dispone de los canales en sitio web.

Teléfono: 3547700.

Correo electrónico: protecciondatos@idea.gov.co.

6. MEDIDAS DE SEGURIDAD DIGITAL

Con el objetivo de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, el IDEA ha implementado medidas técnicas, humanas y administrativas buscando la seguridad de los registros mitigando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, y mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje, la implementación de medidas de seguridad que busquen la confidencialidad, integridad y disponibilidad de la información en el tratamiento de los datos personales.

Las medidas tomadas para la seguridad digital por el IDEA son las siguientes:

Estableció un Sistema de Gestión de Ciberseguridad, Seguridad de la Información y Protección de Datos personales tomando como guía los estándares de la familia ISO 27000, los recomendados por el Instituto Nacional de Tecnología y Estándares (NIST, por sus siglas en inglés) y el Modelo de Seguridad y Privacidad de la Información (MSPI) recomendado por la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

En caso de incidentes cibernéticos graves o muy graves, conforme con los criterios del sistema de gestión establecido y el tipo de afectación, el Instituto reportará, por tardar dentro de las 24 horas siguientes a su acontecimiento, al CSIRT-Gobierno y/o a la Superintendencia de Industria y Comercio.

El IDEA Implementa controles de seguridad durante el ciclo de vida del desarrollo de software.

Implementar controles de seguridad relacionados con la autenticación, definición de roles y privilegios y separación de funciones.

Se exigen estas mismas medidas de seguridad a los proveedores del hosting.

Aplicación de mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.

Proteger la integridad del código, mediante:

1) Validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get)
2) Cookies (habilitar atributos de seguridad como Secure y HttpOnly)
3) Cabeceras HTTP.
4) Sanitización de los parámetros de entrada.
5) Eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos.
6) Sanitización y aseguramiento de variables en el código.
7) Verificación estándar de las Políticas de Origen de las cabeceras.
8) Verificación y comprobación del token de CSRF (cuando aplique).
9) Ejecutar monitoreos de seguridad sobre los sitios web que contemple, entre otras, las siguientes acciones:
10) Escaneo de archivos.
11) Análisis de vulnerabilidades.
12) Análisis de patrones para detectar acciones sospechosas
13) Verificación contra listas negras.
14) Monitoreo del tráfico para detectar ataques de denegación de servicios.
15) Se exigen mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y se solicitan renovaciones periódicas de las mismas garantizando la accesibilidad de personas con discapacidad.
16) Mantener actualizado el software, frameworks y plugins de los sitios web.
17) Restringir el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.
18) Ocultar y restringir páginas de acceso administrativo.
19) Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.
20) Crear copias de respaldo.
21) Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.
22) Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales

transaccionales, para evitar la manipulación de parámetros en las peticiones (adicional al cifrado SSL).

23) Habilitar las cabeceras de seguridad, entre otras las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Strict-Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature-Policy.

24) Implementar mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas, incluyendo la accesibilidad para las personas con discapacidad.

25) Proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación.

26) Sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script», además de la restricción de formatos y tamaños para subida de archivos.

27) Sanitización de caracteres especiales (Aseguramiento de variables en el código de Programación).

28) Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Project (OWASP).

29) Implementar en los servidores los controles necesarios (hardware o software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.

30) Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.

31) Remediación de vulnerabilidades.

32) El Instituto cuenta con sus debidos planes de contingencia, DRP y BCP, que permiten garantizar la continuidad acorde a los niveles de servicio establecidos para cada sitio.

33) Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.

34) Implementar sistemas antivirus en los servidores, para garantizar medidas contra infecciones de malware.

35) Controlar el escalamiento de privilegios en los Sistemas Operativos, servidores web y Bases de datos que hacen parte de la infraestructura.

7. PROGRAMACIÓN DEL CÓDIGO FUENTE

El IDEA en todos sus sitios web, móvil y aplicaciones implementa estándares de desarrollo seguro para evitar vulnerabilidades en el código fuente y errores de presentación o alteraciones en el contenido de la información dispuesta al público. Así mismo, se evitarán mecanismos que puedan poner en riesgo la información o los datos personales o sensibles.

Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones.

Cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C (World Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios.

Adoptar validadores HTML y CCS para la continua revisión del sitio web y su mejora continua, a través de las buenas prácticas del W3C (World Web Wide Consortium).

Incluir lenguaje común de intercambio para la generación y divulgación de la información y datos estructurados y no estructurados dispuestos en medios electrónicos.

Implementar un sistema de control de versiones (Git), que permitan planear y controlar la vida de la aplicación, y en una fase a mediano plazo poder implementar un sistema de integración, cambio y despliegue continuo.