uesvalle
Unidad Educativa del Sur del Valle del Cauca

MAPA Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL

CODIGO	C-DS-13
VERSIÓN	1.0
FECHA	Abril 09 de 2019
PAGINA	1 de 1

IDENTIFICACIÓN DEL RIESGO								VALORACIÓN DEL RIESGO INHERENTE			EVALUACION DE LOS CONTROLES EXISTENTES	NIVEL DE RIESGO RESIDUAL	TRATAMIENTO DE RIESGO RESIDUAL					
NUMERO	NOMBRE DEL PROCESO QUE APLICA	RIESGO DE SEGURIDAD DIGITAL	TIPO DE ACTIVO	DESCRIPCION DEL ACTIVO	TIPO Y DESCRIPCION DE LA AMENAZA	TIPO Y VULNERABILIDAD	CONSECUENCIAS	Probabilidad	Impacto	Zona del riesgo			Opción (es) de Manejo	Actividad de control	Soporte	Responsable	Tiempo	Indicador
1	Gestión Informática	Base de Datos de SYSMAN (Pérdida de la Confidencialidad)	Información	Base de datos con información de procesos de Administrativos y Nomina de la entidad Ley 1712 de 2014 -(Información Reservada) Ley 1581 de 2012-(Contiene datos Personales) Descripción del Riesgo: Pérdida de Datos por modificación, alteración y eliminación de información de la base de datos de nómina de entidad.	Interno Falsificación de Permiso / Derechos Origen: (D-Deliberada,F-Forzuto)	Software 1-Ausencia de Mecanismos de identificación y autentificacion, como la autentificacion de Usuario. 2- Gestión deficiente de las contraseñas.	Pérdida de Dinero, Retraso en el Pago de Nomina, Demandas por incumplimiento de salarios, Plan tortuga de funcionarios, Generación de desconfianza a los ciudadanos.	Posible 3	Mayor 4	Alto 12	Moderado	Moderado 6	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de integridad con relacion a la base de datos de SYSMAN A9.2.4 Gestión de información de autenticacióndde Secreta de Usuarios. Control: la asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. A9.4.3 Sistema de Gestión de contraseñas. Control: Los sistemas de gestión de contraseñas deberían ser interativos y deberían asegurar la calidad de las contraseñas.	Politica de Autenticación de Usuarios (Implementacion del Directorio Activo) - Formulario para la administración de usuarios Nuevos, activos e inactivos (F-GI-06)	Responsable de Proceso	Trimestral (3 meses)	
2	Gestión Informática	Base de Datos de SISA (Pérdida de la Confidencialidad)	Información	Base de datos con información relacionado a los procesos Misionales de la Entidad. Ley 1712 de 2014 -(Información Reservada) Ley 1581 de 2012-(Contiene datos Personales). Descripción del Riesgo: Pérdida de Datos por modificación, alteración y eliminación de información de la base de datos misionales de la entidad.	Interno Falsificación de Permiso / Derechos Origen: (D-Deliberada,F-Forzuto)	Software 1-Ausencia de Mecanismos de identificación y autentificacion, como la autentificacion de Usuario. 2- Gestión deficiente de las contraseñas.	Pérdida de programacion en la area operativa , Retraso en el pago con relacion al reporte de vistas realizadas por la area tecnica. Retraso en el registro de la información realizada por los tecnicos. Demandas por incumplimiento en la no realizacion de las visitas tecnicas.	Posible 3	Mayor 4	Alto 12	Moderado	Moderado 6	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de integridad con relacion a la base de datos de SISA: A9.2.4 Gestión de información de autenticacióndde Secreta de Usuarios. Control: la asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. A9.4.3 Sistema de Gestión de contraseñas. Control: Los sistemas de gestión de contraseñas deberían ser interativos y deberían asegurar la calidad de las contraseñas.	Politica de Autenticación de Usuarios (Implementacion del Directorio Activo) - Formulario para la administración de usuarios Nuevos, activos e inactivos (F-GI-06)	Responsable de Proceso	Trimestral (3 meses)	
3	Gestión Informática	Base de Datos de INFOMED (Pérdida de la Confidencialidad)	Información	Base de Datos con información relacionada a los establecimientos que comercializan o distribuyen los medicamentos de control especial para el departamento del valle del cauca. Ley 1712 de 2014 -(Información Reservada) Ley 1581 de 2012-(Contiene datos Personales) Descripción del Riesgo: Pérdida de Datos por modificación, alteración y eliminación de información relacionada a los medicamentos de control especial (Mayoristas/Minoristas) que se almacenan en la base de datos de entidad.	Interno Falsificación de Permiso / Derechos Origen: (D-Deliberada,F-Forzuto)	Software 1-Ausencia de Mecanismos de identificación y autentificacion, como la autentificacion de Usuario. 2- Gestión deficiente de las contraseñas.	Pérdida de los registros con relacion a los establecimientos obligadotios a reportar los medicamentos de control especial . Demas o cancelacion de contrato por incumplimiento a las funciones misionales con relacion a los comrcios a establecimiento que comercalizan o distribuyen medicamentos de control especial	Posible 3	Mayor 4	Alto 12	Moderado	Moderado 6	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de integridad con relacion a la base de datos de INFOMED. A9.2.4 Gestión de información de autenticacióndde Secreta de Usuarios. Control: la asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. A9.4.3 Sistema de Gestión de contraseñas. Control: Los sistemas de gestión de contraseñas deberían ser interativos y deberían asegurar la calidad de las contraseñas.	Politica de Autenticación de Usuarios (Implementacion del Directorio Activo) - Formulario para la administración de usuarios Nuevos, activos e inactivos (F-GI-06)	Responsable de Proceso	Trimestral (3 meses)	
4	Gestión Informática	Servidor de Base de Datos de SYSMAN (Pérdida de la Confidencialidad)	Hardware	Se encuentra en una Maquina/Virtualizado HP-x44 simultaneo un Servidor Virtualizado hp Proliant Gen 8, Ram 16 GB CPU Xeon 4 Nucleos, Disco Duro 2T Descripción del Riesgo: Acceso no Autorizado al Servidor	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	Hardware 1-Conexión de red pública sin protección. 2-Arquitectura Insegura de la red. 3-Ausencia de Mecanismos de identificación, como la autenticación de usuarios	Ausencia de un eficiente control de cambios en la configuración explotación de vulnerabilidades por falta de actualizaciones de seguridad y hardening .	Probable 4	Mayor 4	Alto 16	Debil	Alto 9	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Confidencialidad con relacion al Servidor de Base de Datos de SYSMAN : A11.1.1 PERIMETRO DE SEGURIDAD fisica : control: se debiera definir y usar perimetros de seguridad, y usarlos para proteger areas que contengan información sensible o critica, instalaciones de manejo de información. A11.1.2 CONTROLES FISICOS DE ENTRADA : Control: las areas seguras se deberian proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. A11.1.3 SEGURIDAD DE OFICINA, RECINTOS E INSTALACIONES: Control: Se debiera diseñar y aplicar seguridad fisica a oficina,recintos e instalaciones A11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES Control: Se debiera diseñar y aplicar proteccion fisica contra desastres naturales, ataques maliciosos o accidentes.	F-GI-02 SOLICITUD DE SOPORTE Y/O SERVICIOS DE SISTEMAS	Responsable de Proceso	Trimestral (3 meses)	
5	Gestión Informática	Servidor de Base de Datos de SISA (Pérdida de la Confidencialidad)	Hardware	Servidor Workstation HP-x440, Ram de 16GB, Disco Duro de 2T,CPU Intel Xeon 4 nucleos. Descripción del Riesgo: Acceso no Autorizado al Servidor	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	Hardware 1-Conexión de red pública sin protección. 2-Arquitectura Insegura de la red. 3-Ausencia de Mecanismos de identificación, como la autenticación de usuarios	Ausencia de un eficiente control de cambios en la configuración explotación de vulnerabilidades por falta de actualizaciones de seguridad y hardening .	Probable 4	Mayor 4	Alto 16	Debil	Alto 9	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Confidencialidad con relacion al Servidor de Base de Datos de SYSMAN : A11.1.1 PERIMETRO DE SEGURIDAD fisica : control: se debiera definir y usar perimetros de seguridad, y usarlos para proteger areas que contengan información sensible o critica, instalaciones de manejo de información. A11.1.2 CONTROLES FISICOS DE ENTRADA : Control: las areas seguras se deberian proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. A11.1.3 SEGURIDAD DE OFICINA, RECINTOS E INSTALACIONES: Control: Se debiera diseñar y aplicar seguridad fisica a oficina,recintos e instalaciones A11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES Control: Se debiera diseñar y aplicar proteccion fisica contra desastres naturales, ataques maliciosos o accidentes.	F-GI-02 SOLICITUD DE SOPORTE Y/O SERVICIOS DE SISTEMAS	Responsable de Proceso	Trimestral (3 meses)	
6	Gestión Informática	Servidor de Base de Datos de INFOMED (Pérdida de la Confidencialidad)	Hardware	Descripción del Riesgo: Acceso no Autorizado al Servidor	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	Hardware 1-Conexión de red pública sin protección. 2-Arquitectura Insegura de la red. 3-Ausencia de Mecanismos de identificación, como la autenticación de usuarios	Ausencia de un eficiente control de cambios en la configuración explotación de vulnerabilidades por falta de actualizaciones de seguridad y hardening .	Probable 4	Mayor 4	Alto 16	Debil	Alto 9	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Confidencialidad con relacion al Servidor de Base de Datos de SYSMAN: A11.1.1 PERIMETRO DE SEGURIDAD fisica : control: se debiera definir y usar perimetros de seguridad, y usarlos para proteger areas que contengan información sensible o critica, instalaciones de manejo de información. A11.1.2 CONTROLES FISICOS DE ENTRADA : Control: las areas seguras se deberian proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. A11.1.3 SEGURIDAD DE OFICINA, RECINTOS E INSTALACIONES: Control: Se debiera diseñar y aplicar seguridad fisica a oficina,recintos e instalaciones A11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES Control: Se debiera diseñar y aplicar proteccion fisica contra desastres naturales, ataques maliciosos o accidentes.	F-GI-02 SOLICITUD DE SOPORTE Y/O SERVICIOS DE SISTEMAS	Responsable de Proceso	Trimestral (3 meses)	Indice de cumplimiento actividades=Número de servicios solucionados sistemas informáticos / Número total de servicios recibidos) X 100
7	Gestión Informática	Aplicativo SISA (Pérdida de la Integridad)	Software	Modificación No autorizada	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	1-Ausencia de Políticas de control de acceso 2-Contraseñas sin Protección 3-Ausencia de mecanismos de identificación y atentication de usuario. 4-Ausencia de bloqueo de sesión	Ausencia de un eficiente control de cambios en la configuración explotación de vulnerabilidades por falta de actualizaciones de seguridad .	Posible 3	Mayor 4	Alto 12	Moderado	Moderado 6	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Integridad con relacion al aplicativo de SYSMAN y sus modulos : A9.2.1 REGISTRO Y CANCELACION DEL REGISTRO DEL USUARIO CONTROL: se debiera implementar un proceso formal de registro y cancelacion de registro de usuarios para posibilitar la asignacion de los derechos de acceso	F-GI-06 FORMULARIO PARA ADMINISTRACIÓN DE USUARIOS NUEVOS,ACTIVOS E INACTIVOS	Responsable de Proceso	Trimestral (3 meses)	
8	Gestión Informática	Aplicativo SYSMAN (Pérdida de la Integridad)	Software	Modificación No autorizada	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	1-Ausencia de Políticas de control de acceso 2-Contraseñas sin Protección 3-Ausencia de mecanismos de identificación y atentication de usuario. 4-Ausencia de bloqueo de sesión	Ausencia de un eficiente control de cambios en la configuración explotación de vulnerabilidades por falta de actualizaciones de seguridad .	Posible 3	Mayor 4	Alto 12	Moderado	Moderado 6	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Integridad con relacion al aplicativo de SYSMAN y sus modulos : A9.2.1 REGISTRO Y CANCELACION DEL REGISTRO DEL USUARIO CONTROL: se debiera implementar un proceso formal de registro y cancelacion de registro de usuarios para posibilitar la asignacion de los derechos de acceso	F-GI-06 FORMULARIO PARA ADMINISTRACIÓN DE USUARIOS NUEVOS,ACTIVOS E INACTIVOS	Responsable de Proceso	Trimestral (3 meses)	
9	Gestión Informática	Aplicativo INFOMED (Pérdida de la Integridad)	Software	Modificación No autorizada	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	1-Ausencia de Políticas de control de acceso 2-Contraseñas sin Protección 3-Ausencia de mecanismos de identificación y atentication de usuario. 4-Ausencia de bloqueo de sesión	Ausencia de un eficiente control de cambios en la configuración explotación de vulnerabilidades por falta de actualizaciones de seguridad .	Posible 3	Mayor 4	Alto 12	Moderado	Moderado 6	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Integridad con relacion al aplicativo de INFOMED y sus modulos : A9.2.1 REGISTRO Y CANCELACION DEL REGISTRO DEL USUARIO CONTROL: se debiera implementar un proceso formal de registro y cancelacion de registro de usuarios para posibilitar la asignacion de los derechos de acceso	F-GI-06 FORMULARIO PARA ADMINISTRACIÓN DE USUARIOS NUEVOS,ACTIVOS E INACTIVOS	Responsable de Proceso	Trimestral (3 meses)	
10	Gestión Informática	Base de Datos de Acta de Avance (Pérdida de la Integridad)	Información	Base de datos en editor XAMM realizada enlazada a una plantilla de Excels y Word. Ley 1712 de 2014 -(Información Reservada) Ley 1581 de 2012-(Contiene datos Personales) Descripción del Riesgo: Pérdida de Datos por modificación, alteración y eliminación de información relacionada a los avances de las actividades contractuales que tiene la entidad.	Interno Falsificacion de Permiso / Derechos	Software 1-Ausencia de Mecanismos de identificación y autentificacion, como la autentificacion de Usuario. 2- Gestión deficiente de las contraseñas.	Atraso en el pago de la nómina datos contratistas, demandas por incumplimiento de salario, pérdida del registro del avance de las actividades contractuales del contratista.	Probable 4	Mayor 4	Alto 16	Moderado	Alto 9	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de integridad con relacion a la base de datos de Acta de avance A9.2.4 Gestión de información de autenticacióndde Secreta de Usuarios. Control: la asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. A9.4.3 Sistema de Gestión de contraseñas. Control: Los sistemas de gestión de contraseñas deberían ser interativos y deberían asegurar la calidad de las contraseñas.	Politica de Autenticación de Usuarios (Implementacion del Directorio Activo) - Formulario para la administración de usuarios Nuevos, activos e inactivos (F-GI-06)	Responsable de Proceso	Trimestral (3 meses)	
11	Gestión Informática	Servidor de Aplicativo Acta de Avance (Pérdida de la Confidencialidad)	Hardware	HP compaq 8300, Ram 8GB, CPU Intel core i7 -3,4hz, Disco duro 1T Descripcion del Riesgo: Acceso no Autorizado al Servidor, donde se encuentra los datos de los contratistas para el pago de sus actividades contractuales	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	Hardware 1-Conexión de red pública sin protección. 2-Arquitectura Insegura de la red. 3-Ausencia de Mecanismos de identificación, como la autenticación de usuarios	1-Desconfianza ciudadanos, Robo de información, cifrado de información (Ramsonware). 2-Robo de información, actuación de Malware, escalamiento de Privilegios, Modificación y Eliminación de datos.	Probable 4	Mayor 4	Alto 16	Moderado	Alto 9	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Confidencialidad con relacion al Servidor aplicativo Acta de Avance A11.1.1 PERIMETRO DE SEGURIDAD fisica : control: se debiera definir y usar perimetros de seguridad, y usarlos para proteger areas que contengan información sensible o critica, instalaciones de manejo de información. A11.1.2 CONTROLES FISICOS DE ENTRADA : Control: las areas seguras se deberian proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. A11.1.3 SEGURIDAD DE OFICINA, RECINTOS E INSTALACIONES: Control: Se debiera diseñar y aplicar seguridad fisica a oficina,recintos e instalaciones A11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES Control: Se debiera diseñar y aplicar proteccion fisica contra desastres naturales, ataques maliciosos o accidentes.	F-GI-02 SOLICITUD DE SOPORTE Y/O SERVICIOS DE SISTEMAS	Responsable de Proceso	Trimestral (3 meses)	
12	Gestión Informática	Aplicativo Acta de Avance (Pérdida de la Integridad)	Software	Modificación no autorizada	Interno Uso no autorizado del Equipo / Falsificacion de Derechos Origen: (D-Deliberada,F-Forzuto)	1-Ausencia de Políticas de control de acceso 2-Contraseñas sin Protección 3-Ausencia de mecanismos de identificación y atentication de usuario. 4-Ausencia de bloqueo de sesión	Ausencia de un eficiente control de cambios en la configuración explotación de vulnerabilidades por falta de actualizaciones de seguridad .	Posible 3	Mayor 3	Alto 9	Moderado	Moderado 4	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Integridad con relacion al aplicativo de Acta de avance y sus modulos : A9.2.1 REGISTRO Y CANCELACION DEL REGISTRO DEL USUARIO CONTROL: Se debería implementar un proceso formal de registro y cancelación de registro de usuarios para posibilitar la asignación de los derechos de acceso.	F-GI-06 FORMULARIO PARA ADMINISTRACIÓN DE USUARIOS NUEVOS,ACTIVOS E INACTIVOS	Responsable de Proceso	Trimestral (3 meses)	
13	Gestión Informática	Infraestructura local.es Deficiente del Data Center (Pérdida de Disponibilidad)	Instalaciones	Servicios no disponibles para el acceso de los datos que existen almacenados dentro de los servidores de la entidad.	Externo Destrucción de los equipos o Medios tecnologicos. Destrucción del Sistema de Cableado	Lugar 1- Ausencia de protección física de las edificación. 2- Arquitectura insegura de la red física. Red 3-conexión deficiente de los cables 4-Arquitectura insegura de la red 5-Ausencia de identificación y autentificación de emisor y receptor. 6-Áreas de comunicación sin protección. 7-conexiones de red pública sin protección	Retrasos en los diferentes procesos estrategicos, misionales y de apoyo de la entidad, demandas o sanciones por incumplimiento del no envio de documentos o archivos ante los entes de control.	Probable 4	Mayor 4	Alto 16	Moderado	Alto 9	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Disponibilidad, con relacion al Data Center : A 11.2.1 Ubicación y Protección Control: El Data Center deberan estar ubicado y protegido para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para el acceso no autorizado. A11.1.1 PERIMETRO DE SEGURIDAD fisica : control: se debiera definir y usar perimetros de seguridad, y usarlos para proteger areas que contengan información sensible o critica, instalaciones de manejo de información. A11.1.2 CONTROLES FISICOS DE ENTRADA : Control: las areas seguras se deberian proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. A11.1.3 SEGURIDAD DE OFICINA, RECINTOS E INSTALACIONES: Control: Se debiera diseñar y aplicar seguridad fisica a oficina,recintos e instalaciones A11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	Plano- Distibucion de Planta.	Responsable de Proceso	12 meses	Elaborar un sistema de seguridad para autenticación e ingreso del personal autorizado
14	Gestión Informática	Portal web (Pérdida de Disponibilidad)	Servicios	Servicio contratado con un proveedor para el portal institucional de la Entidad. Descripción del Riesgo: Servidor fuera de servicio, impidiendo que los usuarios autorizados no tengan acceso para publicación o modificación de información o documentación legal de la Entidad.	Externo Pérdida de disponibilidad portal web	Software 1-Contraseñas sin Protección.	Robo o Pérdida de la información, publicaciones fraudulentas,suplantacion de identidad .	Posible 3	Mayor 3	Alto 9	Moderado	Moderado 4	Reducir el Riesgo	El propósito de las actividades de control que se desarrollan buscan prevenir las causas que puedan dar origen al riesgo de Pérdida de la Disponibilidad , con relacion al Portal WEB : A9.4.3 Sistema de Gestión de contraseñas. Control: Los sistemas de gestión de contraseñas deberían ser interativos y deberían asegurar la calidad de las contraseñas.	F-GI-06 FORMULARIO PARA ADMINISTRACIÓN DE USUARIOS NUEVOS,ACTIVOS E INACTIVOS. F-GI-03 SOLICITUD DE MODIFICACION Y/O CARGA DE LA Información EN EL PORTAL WEB DE LA UES VALLE .	Responsable de Proceso	Trimestral (3 meses)	Inspeccionar los controles de acceso de los usuarios registrados. Número de publicaciones extenas subidas a la página web / Número total de publicaciones solicitadas X 100