



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE
DUITAMA

EMPODUITAMA SA. ESP

“CUIDA LA VIBRANTE ESCENCIA DE LA VIDA”

***PLAN DE TRATAMIENTO DE RIESGOS DE
SEGURIDAD Y PRIVACIDAD DE LA
INFORMACION***

2019



EMPODUITAMA S.A. E.S.P TEL. 098 7602711
EDIFICIO MULTICENTRO TEL. 098 7604400
DUITAMA COLOMBIA FAX. 098 7605304
CALLE 16 14-68 E. empoduitama@hotmail.com

Contenido

| | |
|---|----------|
| INTRODUCCION | 3 |
| 2. OBJETIVOS | 3 |
| 2.1. Objetivo General | 3 |
| 2.2 Objetivos específicos | 3 |
| 3. ALCANCE | 3 |
| 4. DEFINICIONES: | 3 |
| 6. POLITICA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES | 8 |
| 7. VALORACIÓN DEL RIESGO EN EL CONTEXTO DE EMPODUITAMA S.A E.S.P. A LOS ACTIVOS DE INFORMACIÓN | 9 |
| 7.1. Contexto estratégico de EMPODUITAMA | 9 |
| 7.2. Contexto de Seguridad y Privacidad de la información | 9 |
| 8. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | 9 |



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

<https://www.pmg-ssi.com/2017/05/iso-27001-plan-de-tratamiento-de-riesgos-de-seguridad-de-la-informacion/>

INTRODUCCION

El presente documento busca generar cultura en cuanto a los riesgos asociados al tratamiento de datos, así como su manejo y la forma de prevenirlo, de esta manera se presentan los riesgos a los cuales pueda estar expuesta la EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P” y la forma en la cual cada uno de los funcionarios que tienen a su cargo el manejo de cualquier tipo de información debe garantizar su adecuado tratamiento.

2. OBJETIVOS

2.1. Objetivo General

2.2 Objetivos específicos

3. ALCANCE

La estructura del plan de tratamiento de riesgo de seguridad y privacidad de la información para los procesos de la EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.”, teniendo en cuenta los recursos con los que actualmente dispone la empresa y alineándolo a las metodologías DAPF e ISO respectivamente en seguridad y riesgo de la información. El alcance de este documento se extiende a todos los procesos que ejecuta la empresa, en especial aquellos en los que se cuenta con información personal de usuarios o colaboradores de la entidad, o información de los procesos misionales buscando mantenerlos resguardados y seguros.

4. DEFINICIONES:

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** 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 y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** 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. (Decreto 1377 de 2013, art 3).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** 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. (Ley 1581 de 2012, art 3)



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** 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. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACION DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- **Alta Dirección:** aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.
- **Proceso Administración del Sistema Integrado de Gestión:** Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.
- **Responsables de los procesos:** Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

- **Servidores públicos y contratistas:** ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.
- **Control Interno:** debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

6. POLITICA DE PROTECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

Con el fin de cumplir con este plan EMPODUITMA se compromete a el cumplimiento de los siguientes puntos, por parte de todos los integrantes del equipo de trabajo de la organización y las partes interesada:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
- c) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- d) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- e) Actualizar la información dentro de los cinco (5) días hábiles contados a partir de su recibo, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
- f) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley.
- g) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley.
- h) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- i) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- j) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
- k) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- l) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.



EMPODUITAMA S.A. E.S.P TEL. 098 7602711
EDIFICIO MULTICENTRO TEL. 098 7604400
DUITAMA COLOMBIA FAX. 098 7605304
CALLE 16 14-68 E. empoduitama@hotmail.com

- m) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

Para el cumplimiento de los puntos anteriores la dirección debe destinar los recursos necesarios en cuanto a los recursos humanos, financieros y tecnológicos, y garantizar el plan de seguimiento y evaluación.

7. VALORACIÓN DEL RIESGO EN EL CONTEXTO DE EMPODUITAMA S.A E.S.P. A LOS ACTIVOS DE INFORMACIÓN

7.1. Contexto estratégico de EMPODUITAMA

EMPODUITAMA S.A. E.S.P. fue creada inicialmente como Empresa de Obras Sanitarias de Duitama Ltda. mediante escritura pública No. 409 de fecha 12 de agosto de 1976 de la Notaría Segunda de Duitama, inscrita en la Cámara de Comercio de Duitama el 08 de septiembre de 1976 bajo el número 277 del Libro IX según consta en el certificado de constitución y gerencia expedido por la Cámara de Comercio de Duitama.

Según acta No. 005 de fecha 29 de agosto de 2007 en reunión extraordinaria del Consejo Directivo y protocolizada con la escritura pública No. 2253 del 04 de septiembre de 2007 se cedieron cuotas partes de interés social y se transformó en sociedad por acciones del tipo de sociedad anónima, adquiriendo la denominación de Empresa de Servicios Públicos Domiciliarios de Duitama S.A. E.S.P. "EMPODUITAMA S.A. E.S.P." Su objeto social principal es la prestación de los servicios públicos esenciales de acueducto y alcantarillado en el área de jurisdicción del municipio de Duitama y facultada para prestar esos mismos servicios en cualquier lugar del ámbito nacional e internacional.

7.2. Contexto de Seguridad y Privacidad de la información

La información de EMPODUITAMA, se considera como un activo decisivo para el desarrollo de sus procesos, su correcto desempeño dentro de la política y su relación con el ciudadano es por ello que debe ser protegida de cualquier posibilidad de eventos que generen un potencial riesgo de seguridad de la información y que pudiese dar como resultado en un impacto indeseado generando una consecuencia negativa para el normal desarrollo de las actividades de la entidad.

8. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

| Riesgo | Descripción | Control |
|--|--|--|
| Daño en el hardware de oficinas de Empoduitama | Daños en computadores, impresoras, tablets y otros equipos de Empoduitama | Equipo de respaldo para solucionar el inconveniente y prodeer al mantenimiento del equipo afectado |
| Ocurrencia de catástrofe de origen natural | Catástrofes como inundaciones, terremotos, tormentas eléctricas pueden afectar la integridad de la información, ya sean registros físicos o lógicos | Copias de seguridad en disco duros externos, La nube y DVD´s |
| Pérdida de suministro de energía, variación de voltaje | Las variaciones de energía pueden causar daños en los equipos de cómputo o pérdidas de datos si no existen fuentes alternas de suministro de energía como UPS | La UPS controla 35 equipos de la red de Empoduitama a los demas se les tiene UPS por equipo |
| Perturbación de servicio de conectividad debido a la radiación | Se refiere a interferencias dadas por dispositivos que emiten ondas electromagnéticas, capaces de interferir con el funcionamiento | Rediseñar la central de datos con pisos que ayuden a la disminución de la radiación |
| Intercepción de correos electrónicos | Posibilidad de que una tercera persona acceda a los correos electrónicos, ya sea por un método informático o el descuido del puesto de trabajo por parte del funcionario | Asignacion de correos por dependencia por parte del administrador del area de sistemas, con cambios de clave a cada usuario. |
| Espionaje remoto | Uso de técnicas informáticas para revisar el contenido de los discos duros de los equipos de cómputo de la entidad | seridores UTM que controlan información de entrada a la red dde Empoduitama, antivirus, antyspam. Se utilizan IP publicas y no se tienen WIFE al publico |
| Hurto de medios o documentos | Robo de documentación valiosa para la entidad en cualquier medio, físico o magnético | Tener sitios aporpiado para dejar elementos (PDA, Impresoras) y no permitir personal que no sea autorizado |



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

| | | |
|---|---|---|
| Hurto de equipos | Robo de equipos de computo con aplicaciones o información de uso exclusivo de Empoduitama con información restringida | Camaras por dependencia con control de grabación |
| Recuperación de medios reciclados o desechados | Uso de memorias, CDs, discos duros, tablets, computadores, etc, que tenían información confidencial. Es necesario formatear 7 veces un dispositivo para borrar completamente todo rastro de información | Tener un plan de manejo para eliminar totalmente la infomracón cuando no se requiera o se paso a otro equipo de computo |
| Datos provenientes de fuentes no confiables en la WEB | Consulta de información en medios no oficiales o no académicos. Ej: Wikipedia, portales diferentes al SECOP | Bloque de pagina por medio del servidores UTM |
| Manipulación de hardware | Cambios en los componentes físicos de computadores, tablets, impresoras, etc, con fines inescrupulosos | Etiquetas de seguridad por equipo que me garantice cuando hay manipulación |
| Manipulación de software | Cambios no autorizados en el código fuente y/o bases de datos de los programas de cómputo con fines inescrupulosos | Se maneja Windowa Server con perfiles de usuarios por medio de un administrador del sistema y red |
| Mal funcionamiento de software | Los programas de cómputo no funcionan como deberían, se puede dar que no cumplan con los requisitos de normatividad actuales o los datos no concuerden con la realidad | Requerimiento al proveedor de las fallas presentadas en el software para que efectue un analisis y solucion al respecto. Auditoria de un externo experto para analisis de los datos |
| Uso no autorizado de los equipos | Ej: Instalación de juegos, navegación en páginas no autorizadas y para fines diferentes a las funciones laborales | Se maneja Windowa Server con perfiles de usuarios por medio de un administrador del sistema y red |



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

| | | |
|---|--|---|
| Uso de software sin licencia | Uso de programas de cómputo que requieren pago sin contar sin los derechos de uso, dentro de los programas de pago más comunes se encuentra: - Adobe reader - Adobe photoshop - Suite de office microsoft (Word, Excel, Power Point) Existen aplicaciones gratuitas que no requieren de licencia | En el momento de la adquisición de equipos de computo verificar las licencias adquiridas instalar unicamente estas. |
| Corrupción de los datos | Se refiere a archivos que se dañan por la migración a otros formatos. Ej: Archivo creado en Word 2003 que se guarda en formato de 2016 | Copias de seguridad en medios extraibles |
| Procesamiento ilegal de los datos | Manipulación de registros (Actualización, borrado intencional, creación) | Auditoria por control interno a dependencias en los software que posee la Empresa. Generar informe de control de cambios por modulo para verificación con los soportes. |
| Intrusión, accesos forzados al sistema | Acceso por terceras personas o personal no autorizado a información restringida, esto se puede dar por descuido del personal, abandono del puesto de trabajo, etc | Bloqueo automatico despues de determinado tiempo en los software adquiridos |
| Suplantación de identidad | Uso de credenciales pertenecientes a otra persona para acceder a información valiosa u otros privilegios | Creacion de usuarios de acuerdo al perfil de la dependencia y funciones |
| Presencia de virus en terminales usadas por contratistas y funcionarios | Entiéndase por terminales los equipos de cómputo, celulares, tablets, etc. | Los equipos externos no se permite ingresarlos a la red de Empoduitama de no ser atorizados por el area de sistemas. |
| Presencia de virus | Presencia de virus en los | Servidro UTM qu em garantiza bloque de |



EMPODUITAMA S.A. E.S.P
EDIFICIO MULTICENTRO
DUITAMA COLOMBIA
CALLE 16 14-68

TEL. 098 7602711
TEL. 098 7604400
FAX. 098 7605304
E. empoduitama@hotmail.com

| | | |
|---|---|---|
| en servidores | equipos que alojan las aplicaciones de la alcaldía | pagina mal intencionadas, firewall, antivirus |
| Ausencia o insuficiencia de pruebas de software | La falta de pruebas lleva a sistemas con errores lo que puede significar, pérdidas e inconsistencia de la información | Realizar copias diarias, analizar casos con el proveedor del software |
| Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo | Posibilidad de dejar sesiones abiertas en aplicaciones, lo que puede llevar a que otras personas que acceden al equipo puedan acceder a información reservada/clasificada o hacer cambios no autorizados | Bloqueo de sesion despues de 05 minutos de no uso del equipo. |
| Ausencia de auditorías | Falta de auditorías para comprobar el estado de la información y las aplicaciones o infraestructura física y lógica que la aloja (integridad, disponibilidad de recursos, uso de disco duro, actualización de la versión que muchas veces corrige fallas de seguridad, etc) | Crear plan para tener auditorias de seguridad, ikntegridad y privacidad de la información |
| No tener control de incendios donde reposan los Servidores | Posibilidad de corto, falla o sobrecarga electrica que genere un incendio donde se encuentran la indformación de la Empresa en los discos duros de los servidores | Tener detector de incenidos |