AUDITORÍA EN SEGURIDAD INFORMÁTICA EN BASE DE DATOS DEL GRUPO DE TRABAJO DE INFRAESTRUCTURA Y SOPORTE DE TECNOLOGÍAS DE LA INFORMACIÓN DEL DEPARTAMENTO PARA LA PROSPERIDAD SOCIAL – DPS – DE BOGOTÁ, SEDE PRINCIPAL

CLAUDIA ANDREA LASSO URBANO

UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2015

AUDITORÍA EN SEGURIDAD INFORMÁTICA EN BASE DE DATOS DEL GRUPO DE TRABAJO DE INFRAESTRUCTURA Y SOPORTE DE TECNOLOGÍAS DE LA INFORMACIÓN DEL DEPARTAMENTO PARA LA PROSPERIDAD SOCIAL – DPS – DE BOGOTÁ, SEDE PRINCIPAL

CLAUDIA ANDREA LASSO URBANO

Proyecto de Investigación

Salomón González García
Asesor de Proyecto

UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2015

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 12 de junio de 2015

Dedicatoria

A mis hijos y esposo quienes soportaron con mucha valentía mi ausencia; a mis padres y demás familiares por brindarme todo su apoyo y confianza.

Agradecimientos

A Dios por la fortaleza, a mi familia por su comprensión, a mis amigos por su preocupación, a mi Director por sus conocimientos y profesionalismo.

CONTENIDO

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

El contenido del presente trabajo refleja el resultado de una auditoría en seguridad informática realizada sobre las bases de datos del Departamento para la Prosperidad Social (DPS) cuyo principal activo es la información relacionada con la identificación de beneficiarios, así como la infraestructura que soporta los sistemas de información y demás servicios involucrados.

El análisis de riesgos se fundamenta en la metodología Magerit, iniciando con un levantamiento de activos los cuales son valorados, se realiza la identificación de amenazas y la definición de salvaguardas, para finalmente realizar un informe con los hallazgos encontrados en cuanto a la efectividad de los controles existentes y las recomendaciones necesarias para la implementación de nuevos controles que garanticen la confiabilidad, disponibilidad y la integridad de la información.

INTRODUCCIÓN

La necesidad de agrupar, clasificar y estandarizar la información que las empresas u organizaciones han recopilado en el transcurso de su operatividad; la masificación de las tecnologías de la información; el uso de dispositivos electrónicos y por supuesto las necesidades de atención al usuario cada vez más eficientes, oportunas y precisas, han dado vida a términos, áreas de estudio y ciencias de la investigación relacionadas con los sistemas de información y las bases de datos.

A cualquier nivel organizacional, la información se ha convertido en un insumo muy importante y en esa misma medida amerita un tratamiento especial en términos de seguridad ya que a medida que se estructuran los procesos y procedimientos, la información crece exponencialmente y las necesidades de consolidación se hacen cada vez más evidentes y necesarias; es por esto que paralelamente se debe trabajar en mantener estos datos con la mayor integridad posible, adicionalmente a los estándares de información que permitirán procesar y reportar información de calidad. Adicionalmente a la información, se debe contar con los medios necesarios para almacenarla y operarla, hablamos en términos de la infraestructura computacional.

La protección de los elementos mencionados (información e infraestructura) es a grandes rasgos lo que abarca la seguridad informática, cuyo objetivo es minimizar los riesgos a los que están expuestos dichos elementos, utilizando para ello diferentes técnicas o teorías especializadas en el tema; adicionalmente y como medio de control para revisión y ajustes en los procedimientos de seguridad, es necesario realizar una verificación mediante auditorías con el fin de establecer el cumplimiento de los procesos implementados.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

El DPS fue creado mediante decreto No. 4155 del 2011, el cual lo transformó de Agencia Presidencial al Departamento Administrativo con el fin de fortalecer la política social y de atención a la población pobre, vulnerable y víctima de la violencia, convirtiéndose en el organismo principal de la administración pública del Sector Administrativo de Inclusión Social y Reconciliación con un total de 1.300 empleados aproximadamente, distribuidos en todo el territorio nacional. Dicha transformación planteó una nueva organización interna a nivel de áreas y grupos de trabajo con el fin de dar soporte a los diferentes programas existentes en la Entidad, así como a la infraestructura tecnológica que la soporta.

Durante este proceso de transformación, el cual llevó más de 2 años, se presentaron traumatismos en la operación normal de la Entidad, la falta de lineamientos, reorganización del personal, bases de conocimiento perdidas por deserción del personal; desestabilizaron de alguna manera los procesos normales que manejaba la Entidad.

Estos inconvenientes se reflejaron específicamente en el área de Sistemas, la cual se vio afectada desde su estructura jerárquica, al eliminar tres grupos de trabajo que abarcaban tareas bien definidas en temas relacionados con desarrollo de software, telecomunicación y soporte técnico a ser una sola oficina diezmada en el número de personal, sin control de lineamientos, políticas, adquisición de elementos o transversalita en los procesos contractuales y encargada únicamente a la parte operativa, teniendo que cumplir con las siguientes actividades:

- Articular con la Oficina de Tecnologías de Información la prestación integrada de servicios tecnológicos que requiere la entidad.
- Gestionar, planificar y controlar el mantenimiento preventivo y correctivo de la infraestructura tecnológica de la entidad.
- Realizar el diseño, desarrollo, mantenimiento y soporte de los sistemas de información, de acuerdo con las necesidades de la Entidad.
- Definir y administrar los niveles de servicios tecnológicos, de conformidad con los requerimientos de las dependencias del Departamento Administrativo para la Prosperidad Social, los procesos y procedimientos establecidos.
- Garantizar la disponibilidad de la plataforma de tecnología y atender los niveles de servicios acordados con los usuarios.
- Prestar los servicios de mesa de ayuda, soporte a usuarios en sitio y solución de problemas
- relacionados con la operación tecnológica.
- Asegurar el correcto funcionamiento de los recursos informáticos.

- Gestionar la adquisición, mantenimiento y la actualización de la plataforma tecnológica, de acuerdo con las tendencias y necesidades de la entidad.
- Proponer e implementar políticas de seguridad informática y planes de contingencia de la
- plataforma tecnológica y supervisar su adecuada y efectiva aplicación.
- Implementar las políticas y estándares definidos por la Oficina de Tecnologías de la Información.
- Mantener en funcionamiento las aplicaciones en producción, mediante la administración de los
- servidores, el sistema operativo, las bases de datos y los servicios de telecomunicaciones.
- Brindar asesoría a las dependencias en la definición y valoración de necesidades tecnológicas.
- Elaborar los informes requeridos por el Subdirector de Operaciones y la Secretaria General.
- Promover y desarrollar continuamente la implementación, mantenimiento y mejora del Modelo
- Integrado de Planeación y Gestión en el Grupo Interno de Trabajo
- Las demás que le sean asignadas de acuerdo con su naturaleza.

A raíz de la falta de controles en los procesos necesarios para el buen funcionamiento de la infraestructura, los cambios administrativos que también debilitaron financieramente al área, desencadenaron la no continuidad de contratos de mantenimiento de la infraestructura lo cual se vio reflejado en varios incidentes que afectaron la integridad de la información

Si el área no implementa los controles necesarios para mantener la infraestructura tecnológica en las mejores condiciones, los sistemas de información no brindarán la oportunidad en el registro y la información sobre los beneficiarios no será confiable ni oportuna, perdiendo notablemente la capacidad en la toma de decisiones al analizar datos reales.

1.2 FORMULACIÓN

¿Cómo se puede determinar el estado de la infraestructura, herramientas tecnológicas y sistemas administrados por el grupo de Infraestructura y Soporte de Tecnologías de Información?

1.3 DESCRIPCIÓN

Uno de los principales activos de información que posee el Departamento para la Prosperidad Social – DPS – se basa en la identificación de usuarios beneficiados de los programas que ofrece la Entidad, siendo sin duda la razón de ser de la misma, ya que fundamenta su funcionamiento en la atención a la población más necesitada del país, brindando ciertas condiciones de mejoramiento en

la calidad de vida de las personas. Adicionalmente la diversidad de programas los cuales atienden a varios grupos poblacionales, ha logrado que quienes se convierten en beneficiarios sean cada vez más, así como ha obligado a los programas a replantear su operatividad con el fin de poder brindar mayor atención y cobertura.

Todas estas circunstancias han logrado un incremento en la atención de un más del 30% que aumentan la bodega de datos, que requieren de mayor infraestructura para su almacenamiento y tratamiento, así como las medidas de seguridad a implementar; esto con el fin de minimizar los riesgos asociados a la pérdida de datos, manipulación y no disponibilidad de los servicios asociados a las bases de datos. Contando con una plataforma tecnológica adecuada, tanto el personal, directivas y usuarios en general podrán contar con datos oportunos, efectivos y eficaces; insumo fundamental para la toma de decisiones a nivel organizacional y para poder dar respuesta a múltiples solicitudes en materia de beneficiarios de los programas que oferta el DPS.

La auditoría en seguridad informática brindará un panorama sobre las condiciones en las que se encuentra la infraestructura tecnológica de bases de datos y controles aplicados en el DPS; bajo qué condiciones el grupo de trabajo está brindando sus servicios y ayudará a establecer los pasos a seguir con el fin de fortalecer los puntos más vulnerables que deben ser atacados, involucrando a las directivas y el personal en general.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Realizar una auditoría en seguridad informática en el grupo de trabajo de *Infraestructura y Soporte de Tecnologías de Información* de la sede principal del Departamento para la Prosperidad Social – DPS - de Bogotá, específicamente en las bases de datos existentes en el Centro de Datos que administra éste grupo.

2.2 OBJETIVOS ESPECÍFICOS

- Realizar un levantamiento de información sobre las condiciones en el que se encuentra el Centro de Datos de la sede principal de la Entidad y la distribución de las bases de datos en los servidores, mediante entrevistas y/o listas de chequeo.
- Determinar los riesgos a los que están expuestas las bases de datos que administra el grupo de trabajo de *Infraestructura y Soporte de Tecnologías de Información* con el fin de mitigar robo, fraude y la pérdida de disponibilidad, privacidad, integridad y confidencialidad.
- Elaborar el plan de auditoría de acuerdo a la información recolectada.
- Realizar la Auditoría en Seguridad Informática en el grupo de Infraestructura y Soporte de TI.
- Analizar los resultados de las debilidades encontradas y definir los controles adecuados.
- Elaborar el informe final de la auditoría.

3. MARCO REFERENCIAL

3.1 MARCO TEÓRICO

El término auditoria data de tiempos remotos en que fue aplicado para que los soberanos realizaran mantenimiento a sus cuentas por escribamos independientes con el fin de asumir medidas para evitar desfalcos. Hasta 1862 la auditoría fue reconocida como profesión bajo la ley británica de sociedades anónimas. Esta profesión creció y floreció en Inglaterra entre los años 1862 y 1905 y se introdujo en estados unidos hacia 1900[1].

Con la auditoría como una profesión y la arrasadora evolución tecnológica que ha obligado a las organizaciones a estar a la vanguardia en estos temas, asociados a las políticas gubernamentales; a finales del siglo XX, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos vitales y necesarios para cualquier organización empresarial la información.

La Informática hoy, está implícita en la gestión integral de la empresa, alberga la información que es el activo más importante de la entidad, la cual bien administrada ayuda a la toma de decisiones y debido a la importancia en el funcionamiento de una empresa, también se aplica el término que nació hace un par de siglos: Auditoría Informática.

Adicionalmente se involucra un nuevo término sobre Seguridad Informática que consiste en asegurar que los recursos informáticos o programas de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización[2].

Al hablar de Auditoría en Seguridad Informática estamos abarcando el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de constatar si sus actividades son correctas y de acuerdo a las normativas informáticas y generales prefijadas en la organización[3].

Específicamente la auditoría en seguridad informática abarca los conceptos de seguridad física y lógica, aspectos técnicos que deben fundamentarse en un sistema que aborde esta tarea de una

---

[1] UF University of Florida. (2012). Marco teórico sobre sistemas, auditoría forense, contabilidad, auditoría y estados financieros.

[2] zegurit.blogspot.com. Proyecto de Seguridad Informática. Disponible en: http://zegurit.blogspot.com/

[3] GuindelSanchez, E. (2009). Calidad y seguridad de la información y auditoría informática

forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.
En el ámbito organizacional, si bien Colombia cuenta con leyes que establecen las generalidades para la regulación de la información, al país le falta mucho recorrido para adoptar medidas prácticas concretas que se conviertan en un tema cultural para las empresas y usuarios y el poder llegar a reglas estándar que apliquen a cualquier empresa, ya que existen normas para sectores específicos como el financiero y telecomunicaciones que son los más propensos a las amenazas. Adicionalmente se atribuye este desconocimiento o falta de apropiación a la falta de conciencia a nivel directivo de los daños que pueden ocasionar los incidentes informáticos.

Aunque el tema de estudio está relacionado con la seguridad informática, es importante aclarar que este término parte fundamental del Sistema de Gestión en Seguridad de la Información, y en este caso particular, se ve la necesidad de realizar una auditoría en seguridad informática con el fin de revisar y evaluar los controles, sistemas, procedimientos de informática, equipos de cómputo, su utilización, eficiencia y seguridad.

3.2 MARCO CONCEPTUAL

Con el fin de ampliar las definiciones asociadas a la seguridad informática, a continuación se detallarán los términos más utilizados en el desarrollo de éste proyecto:

Activo de información: Elemento tangible o no que tiene valor para una organización (NTC-ISO/IEC 27002, 2007).

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a los que están expuestos la organización (Magerit Libro I, 2012, p. 9).

Amenaza: Cualquier evento que pueda provocar daño a la información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo (Suarez, 2013, p. 44).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de verificar el cumplimiento de requisitos (NTC-ISO 19011, 2002).

Base de datos: Conjunto de datos organizados de manera sistemática de tal forma que facilitan su acceso, mantenimiento y unificación. La información que almacenan las bases de datos pueden ser asociados a servicios, elementos, personas o cualquier tipo de dato (Hernández, 2006, p. 154).

Confidencialidad: El uso de la información está restringido al personal debidamente autorizado (Mavixel.com, 2014).

Controles: Métodos, sistemas y procedimientos, que en forma ordenada, se adoptan en una organización, para asegurar la protección de todos sus recursos (NTC-ISO/IEC 27002, 2007).

Disponibilidad: La información debe estar disponible en el momento en que sea requerida sin presentar interrupciones en el normal funcionamiento de los procesos (Mavixel.com, 2014).

Incidente de seguridad: Cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza (NTC-ISO/IEC 27002, 2007).

Información: Conjunto de datos propios que se gestionan y se intercambian entre personas y/o máquinas dentro de una organización (Definicionabc.com, 2015).

Integridad: Garantiza que la información no ha sufrido ninguna clase de modificación durante su recorrido (Mavixel.com, 2014).

Magerit: Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España (Suarez, 2013, p. 45).

Normas ISO: La ISO (International Standarization Organization), como su nombre lo indica es la organización encargada de la normalización o estandarización de normas de tal forma que puedan ser aplicadas a nivel internacional obteniendo efectividad en los procesos y reducción de los costos asociados (Suarez, 2013, p. 28).

Riesgo: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático, causando un impacto en la empresa (Magerit Libro I, 2012, p. 9).

Salvaguarda: Medida de protección que garantiza la disminución de un riesgo (Magerit Libro I, 2012, p. 19).

Seguridad de la Información: Acciones preventivas a nivel tecnológico que permiten garantizar la protección de información (Hernández, 2006, p. 154).

Seguridad Informática: Técnicas desarrolladas para proteger los equipos informáticos y la información de daños accidentales o intencionados (Hernández, 2006, p. 160).

SGSI: Sistema de Gestión de la Seguridad de la Información. Conjunto de políticas para el diseño, implementación y mantenimiento de los controles necesarios para garantizar la seguridad de la información minimizando los riesgos a los que está expuesta (NTC-ISO-IEC 27001, 2013).

Vulnerabilidad: Debilidad en los sistemas que puedan permitir a las amenazas causarles daños y producir pérdidas (Suarez, 2013, p. 44).

3.3 ESTADO ACTUAL

Teniendo como marco de referencia la creación del Departamento para la Prosperidad Social bajo el decreto 4155 de 2011 en donde se legitima el objetivo de formular, adoptar, dirigir, coordinar y ejecutar políticas, planes generales, programas y proyectos para la superación de la pobreza, la inclusión social, la reconciliación, la recuperación de territorios, la atención a grupos vulnerables y reintegración social (Decreto No. 4155, 2011).

Considerando la operatividad de la entidad, la cual establece diversos programas que apoyan la población a nivel nacional que cumplen con ciertas condiciones de vulnerabilidad, se establecen diversas fuentes de información asociados a sistemas de información con datos sensibles de los beneficiarios de la entidad. Dada la importancia y criticidad de esta información, se ha establecido una estructura tecnológica que da soporte a más de 1200 usuarios a nivel nacional, con diversos servicios como sistema de almacenamiento, backup y centralización de la información.

Aunque se han implementado algunos controles para garantizar la seguridad de la información, por reestructuración y cambios administrativos, se ha desmejorado toda la plataforma que existía inicialmente, llegando a un punto de no contar con servicios de mantenimiento básicos lo que ha afectado el buen desempeño del centro de datos y la continuidad de los servicios.

Si bien la entidad se encuentra certificada en el sistema de gestión integral, la parte de seguridad de la información se ha venido desarrollando con la implementación de controles en la medida en que se requiere, no con una estructura o metodología específica y en este punto, no es claro que se encuentra implementado y su funcionamiento.

4. ACTIVOS DE INFORMACIÓN

El levantamiento preliminar de la información se basa en el enfoque basado en procesos de la norma ISO 27001 para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Sistema de Gestión de Seguridad de la Información – SGSI, estimulando la implementación y operación de controles que permitan manejar los riesgos de seguridad asociados a la organización. En este contexto la auditoría en seguridad informática está implícita en el modelo PHVA adoptado por la entidad caso de estudio en su proceso de implementación del SGSI.

Para realizar un diagnóstico de las condiciones en que se encuentra tanto el centro de datos como las bases de datos de Infraestructura y Soporte de Tecnologías de Información de la Entidad, se complementa el inventario de activos levantado por el área diferenciando los siguientes tipos: Equipos informáticos (hardware), Información o datos, Personas, Servicios y Aplicaciones informáticas (Software). Adicionalmente se establece su descripción y si se encuentra actualmente en funcionamiento o no.

Tabla1. Inventario de activos

Tipo de Activo	Nombre del Activo	Descripción del Activo	En funcionamiento
Servicios	Servicio SIBAS	Sistema de información de beneficiarios de Acción Social	Si
Servicios	Servicio ASTREA	Tutelas, asignaciones, respuestas	Si
Servicios	Servicio Masfamilias	Sistema de información de más familias en acción	Si
Servicios	Servicio SIJA	Jóvenes en Acción	Si
Servicios	Servicio ATENEA	Ingreso para la Prosperidad Social	Si
Servicios	Servicio SyM (Resa)	Seguimiento y monitoreo	Si
Servicios	Servicio SIGIE	Sistema de información de Generación de Ingresos y Empleabilidad	Si
Servicios	Servicio SITT	Sistema de Información Trabajemos Todos	Si
Servicios	Servicio DIPS	Dirección de Inclusión Productiva y Sostenibilidad	No
Servicios	Servicio de gestión documental	Orfeo	Si
Servicios	Servicio KACTUS	Sistema de nómina	Si
Servicios	Servicio SICON	Sistema de Información de contratistas	Si
Servicios	Servicio de correo electrónico	Medio de comunicación empresarial	Si
Servicios	Servicio ISOLUCION	Seguimiento a No conformidades	Si
Servicios	Servicio PaginaWeb	Página www.dps.gov.co	Si
Servicios	Servicio Intranet	Red privada de la entidad	Si
Servicios	Servicio SyM Infraestructura	Seguimiento y monitoreo	No
Servicios	Servicio PCT	Sistema financiera y de recursos físicos	Si
Servicios	Servicio SID	Sistema de Información de Donaciones	No
Servicios	Servicio SIAP	Sistema de Información Activos para la Prosperidad	Si
Servicios	Servicio SIOPSR	Sistema de Información Operación Prolongada de Socorro y Recuperación	No
Servicios	Servicio de viáticos	Viáticos y comisiones	No
Servicios	Servicio de Ulises	Viáticos y comisiones	Si

Tabla 1. (Continuación)

Tipo de Activo	Nombre del Activo	Descripción del Activo	En funcionamiento
Servicios	Servicio SOLSIREH	Sistema anterior de nómina	No
Servicios	Servicio Atlas Interactivo	Visor Web	Si
Servicios	Servicio Registros Administrativos	Capturador de Registros Administrativos	Si
Servicios	Servicio de HelpDesk	Dexon	Si
Servicios	Servicio de Consulta de Imágenes	Orfeo	Si
Hardware	Servidor web SIBAS	192.168.2.155 192.168.2.220 VM:nore.dps.gov.coHost:toli.accionsocial.col	Si
Hardware	Servidor BLADE (DB) SIBAS	192.168.0.40 Host: dion.dps.gov.co instancia: masfamilias	Si
Hardware	Servidor web ASTREA	192.168.2.92 VM:nac.accionsocial.colHost:riyer.accionsocial.col	Si
Hardware	Servidor BLADE (DB) ASTREA	Host:cefal.accionsocial.colinstancia:DPS mace: Tutelas 192.168.0.33	Si
Hardware	Servidor web	PUBLICACION DE CONTENIDOS SIFA 192.168.3.63 VM:masfamilias.dps.gov.coHost:rapos.accionsocial.col	Si
Hardware	Servidor web	PUBLICACION DE CONTENIDOS SIFA 192.168.3.66 VM:muchomasfamilias.accionsocial.col Host:	Si
Hardware	Servidor web	PUBLICACION DE CONTENIDOS SIFA 192.168.3.61 VM:masfama2.accionsocial.col Host:	Si
Hardware	Servidor BLADE (PUBLICACION DE CONTENIDOS SIJA)	192.168.3.73 - VM:sofo.accionsocial.colHost:vner.accionsocial.col	Si
Hardware	Servidor BLADE (DB SIJA)	192.168.0.40 host:dion.accionsocial.col	Si
Hardware	Servidor BLADE (PUBLICACION DE CONTENIDOS ATENEA)	192.168.2.192 - VM: rine.accionsocial.colHost:disa.accionsocial.col	Si
Hardware	Servidor BLADE (DB ATENEA)	host: cefal.accionsocial.col instancia: DPS mace:ingresosocial	Si
Hardware	Servidor web SyM (Resa)	192.168.2.185/resa - VM: rine.accionsocial.colHost:disa.accionsocial.col	Si
Hardware	Servidor BLADE SyM DB (Resa)	host:cefal.accionsocial.col	Si
Hardware	Servidor web - SIGIE	Sistema de información de Generación de Ingresos y Empleabilidad 192.168.3.36 - VM: sthenaci.accionsocial.colHost:nepa.accionsocial.col	Si
Hardware	Servidor Database - SIGIE	Sistema de información de Generación de Ingresos y Empleabilidad- 192.168.0.33 host:cefal.accionsocial.col	Si
Hardware	Servidor web SITT	Sistema de Información Trabajemos Todos 192.168.3.36/ETTrabajemostodos - VM: sthenaci.accionsocial.colHost:nepa.accionsocial.col	Si
Hardware	Servidor Databse SITT	Sistema de Información Trabajemos Todos DB: 192.168.0.33 host: cefal.accionsocial.col	Si
Hardware	Servidor web DIPS	Dirección de Inclusión Productiva y Sostenibilidad VM: sthenaci.accionsocial.colHost:nepa.accionsocial.col	No
Hardware	Servidor Databse DIPS	Dirección de Inclusión Productiva y Sostenibilidad DB: 192.168.0.33 host: cefal.accionsocial.col	No
Hardware	Servidor gestión documental (Orfeo)	192.168.2.205 VM:orfeootros.accionsocial.colHost:decha.accionsocial.col	Si
Hardware	Servidor gestión documental (Orfeo) DB	DB: 192.168.0.33 host: cefal.accionsocial.col	Si
Hardware	Servidor KACTUS	192.168.3.77 VM:sofo.accionsocial.colHost:vner.accionsocial.col	Si
Hardware	Servidor KACTUS DB	192.168.0.33 host:cefal.accionsocial.col instancia: administrativa	Si
Hardware	Servidor SICON	192.168.2.239 M:nac.accionsocial.colHost:riyer.accionsocial.col	Si

Tabla 1. (Continuación)

Tipo de Activo	Nombre del Activo	Descripción del Activo	En funcionamiento
Hardware	Servidor database SICON	192.168.2.208 VM: ostos.accionsocial.col Host: julius.accionsocial.col	Si
Hardware	Servidor database correo electrónico	VM1:JANUS.accionsocial.col, VM2:JANUSS.accionsocial.col Host1:mercurio.accionsocial.col Host2:vneptos.accionsocial.col	Si
Hardware	Servidor correo electrónicounifiedmanagement	VMtarvos.accionsocial.col Host: riyer.accionsocial.col	Si
Hardware	Firewall	perimetral/interno	Si
Hardware	Servidor web ISOLUCION	192.168.3.111 - VM: alborix.accionsocial.col Host: decha.accionsocial.col	Si
Hardware	Servidor BLADE (DB) ISOLUCION	Host:julius.accionsocial.colVM:ostos.accionsocial.coldbname:isolucion 192.168.2.208	Si
Hardware	Servidor PaginaWeb	192.168.2.2 VM:rine.accionsocial.col Host: disa.accionsocial.col	Si
Hardware	Servidor BLADE (DB) PaginaWeb	Host:julius.accionsocial.colVM:ostos.accionsocial.coldbname:paginaccionsocial 192.168.2.208	Si
Hardware	Servidor Intranet	192.168.2.54 VM:rine.accionsocial.col Host: disa.accionsocial.col	Si
Hardware	Servidor BLADE (DB) Intranet	Host:julius.accionsocial.colVM:ostos.accionsocial.coldbname: 192.168.2.208	Si
Hardware	Servidor web (SyM Infraestructura)	192.168.2.185/infraestructura - VM: rine.accionsocial.colHost:disa.accionsocial.col	No
Hardware	Servidor BLADE (SyM Infraestructura) DB	host:cefal.accionsocial.col	No
Hardware	Servidor PCT	192.168.2.41 VM: lena.accionsocial.colHost:soco.accionsocial.col	Si
Hardware	Servidor PCT Database	192.168.0.33 host:cefal.accionsocial.col instancia: PCTN	Si
Hardware	Servidor SID	192.168.2.88 VM:core.accionsocial.col Host: disa.accionsocial.col	No
Hardware	Servidor Database SID	192.168.0.33 host: cefal.accionsocial.col	No
Hardware	Servidor SIAP	192.168.2.26 VM:telesto.accionsocial.col Host: toli.accionsocial.col	Si
Hardware	Servidor DB	192.168.0.33 host: cefal.accionsocial.col	
Hardware	Servidor web SIOPSR	Sistema de Información Operación Prolongada de Socorro y Recuperación - 192.168.2.223 VM:nac.accionsocial.col Host: riyer.accionsocial.col	No
Hardware	Servidor BLADE (SIOPSR)	192.168.0.33 host: cefal.accionsocial.col	No
Hardware	Servidor viáticos	192.168.2.49 VM: core.accionsocial.colHost:disa.accionsocial.col	No
Hardware	Servidor viáticos	DB 192.168.2.208 VM:ostos.accionsocial.colHost:julius.accionsocial.col	No
Hardware	Servidor ULISES	192.168.3.32 VM: nac.accionsocial.col Host: riyer.accionsocial.col	Si
Hardware	Servidor ULISES	DB 192.168.2.208 VM:ostos.accionsocial.colHost:julius.accionsocial.col	Si
Hardware	Servidor SOLSIREH	Sistema anterior de nómina	No
Hardware	Server web Atlas Interactivo	192.168.2.28 VM:nac.accionsocial.col Host: riyer.accionsocial.col	Si
Hardware	Server database Atlas Interactivo	192.168.0.33 host: cefal.accionsocial.col	Si
Hardware	Sistema de aire acondicionado	Potencia de enfriamiento de 60000 BTU	Si
Hardware	Array	EVA4000 Storage	Si

Tabla 1. (Continuación)

Tipo de Activo	Nombre del Activo	Descripción del Activo	En funcionamiento
Hardware	Array	EVA6400 Storage	Si
Hardware	Servidor controlador de domino	TITAN.accionsocial.col	Si
Hardware	Switch	Catalyst 3750 Core	Si
Hardware	OpenScapeVoice	Sistema de comunicación de voz	No
Hardware	Servidor BLADE (DB)	Host:cefal.accionsocial.colinstancia:DPS mace: Registrosadmin 192.168.0.33	Si
Hardware	Servidor web	192.168.2.50/servicedesk VM: lena.accionsocial.col Help Desk Host: soco.accionsocial.dps	Si
Hardware	Base de datos dexon.accionsocial.col	192.168.2.204 VM :fedora.accionsocial.col Host: soco.accionsocial.col	Si
Hardware	Sistema contra incendios	Sistema de defensa contra incendios Fm200	Si
Hardware	Servidor web (Sistema de Consulta de Imágenes)	192.168.2.41 VM: lena.accionsocial.col Host soco.accionsocial.col	Si
Hardware	Servidor BLADE (DB Sistema de consulta de imágenes)	192.168.2.25 VM:sinope.acciosocial.colHost:toli.accionsocial.col	Si
Software	Software Sistema de Información SIBAS	Sistema de Información Beneficiarios de Acción Social	Si
Software	Software Sistema de Información ASTREA	Tutelas, asignaciones, respuestas	Si
Software	Software SIFA	Sistema de Información Familias en Acción	Si
Software	Software SIJA	Jóvenes en Acción	Si
Software	Software ATENEA	Ingreso para la Prosperidad Social	Si
Software	Software SyM (Resa)	Seguimiento y monitoreo	Si
Software	Software SIGIE	Sistema de información de Generación de Ingresos y Empleabilidad	Si
Software	Software SITT	Sistema de Información Trabajemos Todos	Si
Software	Software DIPS	Dirección de Inclusión Productiva y Sostenibilidad	No
Software	Software gestión documental	Orfeo	Si
Software	Software KACTUS	Sistema de nómina	Si
Software	Software SICON	192.168.2.239 VM:nac.accionsocial.colHost:riyer.accionsocial.col	Si
Software	Software de correo electrónico	Medio de comunicación empresarial	Si
Software	Software Sistema de Información ISOLUCION	Sistema de No conformidades	Si
Software	Software PaginaWeb	Página www.dps.gov.co	Si
Software	Software Intranet	Red privada de la entidad	Si
Software	Software SyM Infraestructura	Seguimiento y monitoreo	No
Software	Software PCT	Sistema financiera y de recursos físicos	Si
Software	Software SID	Sistema de Información de Donaciones	No
Software	Software SIAP	Sistema de Información Activos para la Prosperidad	Si
Software	Software SIOPSR	Sistema de Información Operación Prolongada de Socorro y Recuperación	No
Software	Software viáticos	Viáticos y comisiones	No
Software	Software ULISES	Viáticos y comisiones	Si
Software	Software SOLSIREH	Sistema anterior de nómina	No
Software	Sistema Atlas Interactivo	Visor Web	Si

Tabla 1. (Continuación)

Tipo de Activo	Nombre del Activo	Descripción del Activo	En funcionamiento
Software	Software Sistema de Información Registros Administrativos	Llave maestra de beneficiarios	Si
Software	Software Sistema de HelpDesk	Dexon	Si
Software	Sistema de Consulta de Imágenes Docuware	Orfeo	Si
Información	Información SIBAS	Sistema de información de beneficiarios de Acción Social	Si
Información	Información ASTREA	Tutelas, asignaciones, respuestas	Si
Información	Información Masfamilias (SIFA)	Sistema de información de familias en acción	Si
Información	Información Jóvenes en Acción (SIJA)	Sistema de información e Jóvenes en acción	Si
Información	Información ATENEA	Sistema de Información de Ingreso Social	Si
Información	Información SyM (Resa)	Seguimiento y monitoreo	Si
Información	Información SIGIE	Sistema de información de Generación de Ingresos y Empleabilidad	Si
Información	Información SITT	Sistema de Información Trabajemos Todos	Si
Información	Información DIPS	Dirección de Inclusión Productiva y Sostenibilidad	No
Información	Información gestión documental	Orfeo	Si
Información	Información KACTUS	Sistema de nómina	Si
Información	Información SICON	Sistema de Información de Contratistas	Si
Información	Información correo electrónico	Medio de comunicación empresarial	Si
Información	Información ISOLUCION	Seguimiento a No conformidades	Si
Información	Información PaginaWeb	Página www.dps.gov.co	Si
Información	Información Intranet	Red privada de la entidad	Si
Información	Información SyM Infraestructura	Seguimiento y monitoreo	No
Información	Información SyM	Paz y Desarrollo	No
Información	Información PCT	Sistema financiera y de recursos físicos	Si
Información	Información - SID	Sistema de Información de Donaciones	No
Información	Información SIAP	Sistema de Información Activos para la Prosperidad	Si
Información	Información SIOPSR	Sistema de Información Operación Prolongada de Socorro y Recuperación	No
Información	Información viáticos	Viáticos y comisiones	No
Información	Información Ulises	Viáticos	Si
Información	Información SOLSIREH	Sistema anterior de nómina	No
Información	Información Atlas Interactivo	Visor Web	Si
Información	Información Registros Administrativos	Llave maestra de beneficiarios	Si
Información	Información Sistema de Consulta de Imágenes	Visor Web	Si
Personal	Oficial de seguridad informática	Responsable de las medidas de seguridad	Si
Personal	Administrador de infraestructura	Responsable de la infraestructura en el centro de datos	Si
Personal	Administrador de Base de Datos	Responsable de la administración del centro de datos	Si

Fuente: Departamento para la Prosperidad Social - DPS

4.1 DISTRIBUCIÓN DE LAS BASES DE DATOS EN LOS SERVIDORES

De acuerdo al alcance del proyecto, se complementa un inventario detallado por servidor de las bases existentes en el Centro de Datos de la Entidad, identificando algunas características técnicas y funcionales:

Tabla 2. Descripción bases de datos

NOMBRE SERVIDOR	DESCRIPCIÓN SERVIDOR	NOMBRE BASE DE DATOS	CARACTERÍSTICAS	MOTOR BASE DE DATOS	TOTAL REGISTROS
DION	Servidor BLADE (DB) SIBAS 172.20.20.40 Host: dion.dps.gov.co instancia: masfamilias	SIBAS	Virtual 62 GB memoria	ORACLE	48.000.000
	Database Oracle 172.20.20.40 host:dion.accionsocial.col	SIFA		ORACLE	18.000.000
	Servidor BLADE (DB SIJA) 172.20.20.40 host:dion.accionsocial.col	SIJA		ORACLE	90.000
FEDORA	Databasesqlserver 172.20.2.204 fedorahost:sinope.accionsocial.col	SIFA	Virtual 20 GB memoria, 8 procesadores	SQL	9.000.000
	Base de datos dexon.accionsocial.col 172.20.2.204 VM :fedora.accionsocial.col Host: coloso.accionsocial.col	DEXON		ORACLE	4.000.000
CEFAL	Servidor BLADE (DB) ASTREA Host:cefal.accionsocial.colinstancia:DPSSchema: Tutelas 172.20.20.33	ASTREA	Virtual 40 GB memoria, 8 procesadores	ORACLE	3.000.000
	Servidor BLADE (DB ATENEA) host: cefal.accionsocial.col instancia: DPS schema:ingresosocial	ATENEA		ORACLE	3.000.000
	Servidor Database - SIGIE (Sistema de informacion de Generación de Ingresos y Empleabilidad)- 172.20.20.33 host:cefal.accionsocial.col	SIGIE		ORACLE	2.000.000
	Servidor Databse SITT (Sistema de Informacion Trabajemos Todos) DB: 172.20.20.33 host: cefal.accionsocial.col	SITT		ORACLE	450.000
	Servidor Databse DIPS (Dirección de Inclusión Productiva y Sostenibilidad) DB: 172.20.20.33 host: cefal.accionsocial.col	DIPS		ORACLE	3.400.000
	Servidor Database SID(Sistema de Informacion de Donaciones) 172.20.20.33 host: cefal.accionsocial.col	SID		ORACLE	230.000
	Servidor DB 172.20.20.33 host: cefal.accionsocial.col	SIAP		ORACLE	340.000
OSTOS	Servidor database SICON 172.20.2.208 VM: ostos.accionsocial.col Host: julius.accionsocial.col	SICON	Virtual 10 GB memoria, 4 procesadores	ORACLE	272.000
JULIUS	Servidor BLADE (DB) ISOLUCION Host:julius.accionsocial.colVM:ostos.accionsocial.coldbname:isolucion 172.20.2.208	ISOLUCION	Físico, 96 GB memoria, 2 procesadores	ORACLE	540.000

Fuente: Departamento para la Prosperidad Social – DPS

- Debido a la naturaleza de los programas que posee la Entidad y especialmente a que se atiende población en condiciones de vulnerabilidad, procurando la reducción de pobreza, desigualdad de ingresos, mejoramiento de condiciones de vida, además de beneficios adicionales como espacios de participación comunitaria; se consideran las siguientes bases de datos como de mayor relevancia por contener datos personales, de ubicación y de beneficios entregados a población específica por parte del Departamento para las Prosperidad Social, adicionalmente a

que son la el insumo para ejercicios de focalización, dar respuesta a infinidad de solicitudes, derechos de petición, estudios y demás análisis de esta población a nivel nacional:

SIFA (Servidor DION y FEDORA):

Almacena toda la información relacionada con Más Familias en Acción que es un programa de transferencias monetarias condicionadas que buscar incentivar la asistencia y permanencia escolar, así como impulsar la atención en salud y buenas prácticas de cuidado en los niños, mujeres, adolescentes y jóvenes(dps.gov.co, 2015). Se cuenta con información histórica desde el 2007 relacionada con el pago de incentivos, en su mayor porcentaje datos de menores bajo la supervisión de un titular o cabeza de familia.

SIJA (Servidor DION):

Programa bajo la misma modalidad de transferencia condicionada que incentiva a los jóvenes a continuar con su educación tanto en el SENA como en otras Instituciones de Educación Superior (dps.gov.co, 2015). Esta base de datos alberga tanto los beneficiarios del programa como los posibles potenciales de ser beneficiarios desde el año 2013.

ATENEA (Servidor CEFAL):

Sistema de información del programa Ingreso para la Prosperidad, el cual surge como respuesta a una de las mayores dificultades que tienen las familias para generar ingresos y radica en las capacidades que les permitan vincularse a una ocupación remunerada o mejorar las condiciones de las actividades que desarrollan, por medio de un incentivo en forma de ingreso que facilite este proceso.

SIGIE, SITT, SID, SIAP, DIPS (Servidor CEFAL):

Contienen información de 8 estrategias en sus diferentes etapas que buscan contribuir al desarrollo de capacidades y del potencial productivo, facilitando el aprovechamiento de oportunidades de empleo, comerciales, el acceso y acumulación de activos, de la población pobre extrema, vulnerable y víctima del desplazamiento forzado por la violencia, con el fin de que pueda lograr una inclusión productiva sostenible (dps.gov.co, 2015).

- Continuando con la importancia de las bases de datos, se destacan aquellas que son insumo para diferentes tipos de consulta directa o por medio de sistemas de información y de cuyos datos depende la focalización de beneficiarios que cumplan ciertas condiciones de acuerdo con la operatividad de cada programa.
  SIBAS (Servidor DION):

Repositorio de datos para fuentes de información externa como Sisben, entre otras, que proporcionan el punto de partida para la selección de los potenciales beneficiarios del Departamento para la Prosperidad Social.

- Finalmente se destacan aquellas bases de datos que apoyan la parte operativa de la Entidad en materia legal y contractual, ya que por su cobertura a nivel nacional, el contacto con entidades gubernamentales territoriales, vinculación con terceros que realizan los trabajos de campo y las disposiciones legales que hacen parte de las obligaciones de la Entidad, la consulta y administración de datos relacionados con estos aspectos debe ser eficiente y oportuna para no incurrir en incumplimientos:

  ASTREA (Servidor CEFAL):

  Sistema de información que administra todos los procesos jurídicos que debe atender la Entidad en temas relacionados con tutelas, reflejando la trazabilidad de cada proceso.

  SICON (Servidor OSTOS):

  Sistema de información relacionada con las etapas contractual y pos contractual de los contratos que adelanta la Entidad por prestación de servicios, operadores que apoyan la ejecución de programas en territorio y demás proveedores de bienes y servicios. El sistema almacena información desde el 2009.

5. SEGURIDAD EN EL CENTRO DE DATOS

Realizado el Checklist (Anexo A), se establecen las condiciones de seguridad existentes en el Centro de Datos de la Entidad:

5.1 ACCESO

El ingreso al Centro de datos se realiza mediante tarjeta electrónica y clave. Se cuenta con una planilla de Entrada/Salida donde el personal tanto interno como externo se registra.

5.2 POLÍTICAS DE SEGURIDAD

No se conocen las políticas asociadas al Centro de Datos.

5.3 MECANISMOS DE PROTECCIÓN/CONTRATOS DE MANTENIMIENTO

Sistema contra incendios: El cual no cuenta con un contrato de mantenimiento y no se ha actualizado desde hace más de dos años.

Sistema de aire acondicionado: No se cuenta con contrato de mantenimiento desde hace aproximadamente un año.

Sistema de réplica: Contrato de RTO (Recovery Time Objetive) con el proveedor de Internet que realiza réplica de aproximadamente 4 aplicaciones.

Adicionalmente se preguntó por los incidentes que hayan ocurrido y las causas que los provocaron, así como otras situaciones anormales:

- Daño de breaker lo que afectó el funcionamiento del sistema de aire acondicionado. Se solicita servicio de mantenimiento a un particular para solucionar el inconveniente, usar otros mecanismos manuales de enfriamiento.

- Cortes de energía. Al no existir planta eléctrica para el Centro de Datos, el funcionamiento de la UPS selimita a una hora y se debe recurrir al apagado de equipos hasta que se restablezca la energía.

- No existen contratos de mantenimiento para el sistema de almacenamiento SAN ni la solución HP enlosare 1-1

- No existe contrato de mantenimiento para las UPS del Centro de Datos y equipos.

Igualmente se indagó sobre los incidentes que hayan ocurrido en el Centro de Datos en el último año:

Daño de Breaker en el aire acondicionado por falta de mantenimiento. Se ataca dejando la puerta abierta del centro de datos, llamando a personal técnico que revisa y soluciona el daño en el momento.

Cortes de energía ya que el centro de datos no cuenta con una planta eléctrica. Se hace un apagado de servidores y se espera hasta que se restablezca la energía ya que la UPS dura solamente 1 hora.

6. SEGURIDAD EN BASES DE DATOS

Realizada la entrevista al DBA de la Entidad, se establecen las condiciones de seguridad existentes sobre las bases de datos de la Entidad:

6.1 MOTORES DE BASES DE DATOS EXISTENTES

SQL Server de las cuales existen varias versiones desdela 2008 hasta la 2014 y Oracle va desde la 11g hasta la 12c. El uso del SQL obedece a la integración de herramientas como Business Intelligence (BI), así como Reporting, Integration y AnalysisServices.

6.2 ANTIVIRUS

Se configuran las políticas de acuerdo a cada motor de base de datos y dependiendo de los archivos a ejecutar. La Entidad cuenta con licencias McAfee actualizado en la versión 8.8 y en las actualizaciones de consola van en la versión 5.1.

6.3 FIREWALL

Las configuraciones se realizan a nivel de servidor. La Entidad cuenta con un firewall a nivel perimetral y uno para los servidores.

6.4 GESTION DE ACCESOS

Las contraseñas son custodia del DBA, se le coloca una política de caducidad de acuerdo al motor, en el caso de Oracle lo asume automáticamente cada 6 meses. En SQL no se aplican políticas de caducidad. No existe una política o procedimiento asociado.

6.5 PROCEDIMIENTOS DE BACKUP

Existe una política actualizada al 2015 la cual incluye en este momento realizar respaldo de los controladores de dominio, servidor de archivos, servidor de correo backend, servidor de correo frontend y bases de datos en SQL y Oracle.

Por cada servidor se establecen las condiciones del Backup, el cual se almacena en cinta magnética y cada 15 días el proveedor de custodia de medios las recoge de acuerdo al esquema establecido, así como un almacenamiento temporal dentro del área. Esto también está soportada por el P*rocedimiento de Ejecución de Backups*y la *Planilla_Control de backups_2013.*

6.6 PROCEDIMIENTOS DE RESTAURACIÓN DE BACKUPS

Existe una política de uso interno que determina como se realiza el procedimiento de backup y las pruebas respectivas de restauración las cuales están soportadas por el *Formato de registro de backups ejecutadas.*

6.7 MANTENIMIENTO BASE DE DATOS

Con el fin de fortalecer el mantenimiento de las bases de datos, el DBA está adelantando un inventario de las mismas, definiendo su criticidad y tiempos de atención; con base en estos resultados se presentarán al Comité de Tecnología con el fin de tomar decisiones importantes y necesarias sobre procedimientos para que los programas informen continuamente los cambios a nivel de aplicativos y responsabilidades asociadas y así poder determinar que bases de datos ya no están en uso y reagrupar con el fin de aprovechar el procesamiento de los servidores.
Sobre las bases de producción, la revisión exhaustiva se realiza cuando se quiera. Igualmente hay tareas automáticas como scripts de encogimiento de logs.

Por la criticidad y alto nivel de consulta y procesamiento para las bases de SIFA, JEA y ATENEA se tienen tareas programadas cada 6 horas para recuperación de BD por recovery, verificar, recoger logs, encoger y elimina los obsoletos. Para el resto de programas se realizan tareas manuales una vez por semana

6.8 SEPARACIÓN DE AMBIENTES

Adicionalmente al inventario de bases de datos se está adelantando en el área un proceso de redistribución de los ambientes tanto de producción como de pruebas ya que no se encuentran aislados en todos los sistemas.

6.9 CONTROL DE ACCESO

El personal de desarrollo solo tiene acceso y ciertos privilegios sobre el ambiente de pruebas. Sobre el ambiente de producción, el DBA es el único con autonomía sobre esas bases. Se mantienen los inconvenientes por independencia de algunos programas en cuanto a los desarrollos y sistemas de información ya que cuentan con personal específico para la administración de los mismos.

6.10 CONCURRENCIA

Como buena práctica el desarrollador debe garantizar el uso de closeconnection al finalizar cada proceso. Aquí intervienen las políticas de conexión a sitios web.

7. ANÁLISIS DE RIESGOS

Proceso metódico que permite analizar actividades o procesos que pueden estar en riesgo en una empresa dando como resultado las medidas de seguridad que deben ser aplicadas para mitigarlos. Existen diversas metodologías para el análisis de riesgos, todas tomando como elementos fundamentales las vulnerabilidades asociadas a los activos de información que pueden aprovechar las amenazas para convertirse en un riesgo inminente de pérdida de información.

Para el caso de estudio se aplicará la metodología Magerit para el análisis y gestión de riesgos, elaborada por el Consejo Superior de Administración Electrónica en su versión 3 actualizada en 2012, la cual contempla los siguientes pasos que concluyen en los riesgos actuales que presenta la empresa relacionados con las bases de datos.

7.1 VALORACIÓN DE LOS ACTIVOS

Se presenta la escala que servirá de referencia para la calificación cualitativa de activos y medir la magnitud de riesgo e impacto:

Tabla 3. Escala valoración de activos

Escala		Valor	Descripción
MB	Muy bajo	1	Irrelevante para la Entidad
B	Bajo	2	Importancia menor
M	Medio	3	Importante
A	Alto	4	Altamente importante
MA	Muy alto	5	De vital importancia para la Entidad

Fuente: Magerit 3.0. Metodología de análisis y Gestión de Riesgos de los Sistemas de Información

Igualmente se definen las dimensiones evaluadas de acuerdo con la importancia de cada activo:

[C] Confiabilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

[I] Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]

[A] Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

[D] Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]

Ya que la Entidad no posee actividades de Ventas por Internet o Comercio electrónica, no se considera la dimensión de [T] Trazabilidad.

Se presenta el resultado de la valoración de activos en el Centro de Datos del Departamento para la Prosperidad Social - DPS:

Tabla4. Valoración de activos

Tipo / Nombre del Activo	Dimensiones			
	[C]	[I]	[A]	[D]
[I] Datos / Información				
Información SIBAS	A	A	A	A
Información ASTREA	M	A	M	A
Información SIFA	A	MA	MA	A
Información SIJA	A	MA	MA	A
Información ATENEA	A	MA	MA	M
Información SyMResa	M	A	MA	A
Información SIGIE	A	A	A	A
Información SITT	A	A	MA	A
Información DIPS	A	A	A	A
Información gestión documental (Orfeo)	MA	A	A	A
Información KACTUS	A	A	MA	A
Información SICON	A	A	A	MA
Información correo electrónico	A	A	M	M
Información ISOLUCION	M	M	M	A
Información Página Web	MB	A	A	A
Información Intranet	M	A	M	M
Información SyM Infraestructura	M	A	M	B
Información SyM Paz y Desarrollo	A	A	M	MB
Información PCT	M	A	A	M
Información SID	B	A	A	B
Información SIAP	B	A	M	A
Información SIOPSR	M	A	M	B
Información Viáticos	M	A	M	M
Información ULISES	M	A	M	M
Información SOLSIREH	A	M	MA	B
Información Atlas Interactivo	MB	A	A	M
Información Registros Administrativos	MB	M	MA	B
Información Sistema de Consulta de Imágenes	MB	MB	MB	MB

Tabla 4. (Continuación)

Tipo / Nombre del Activo	Dimensiones			
	[C]	[I]	[A]	[D]
[S] servicios				
Servicio SIBAS	A	A	A	A
Servicio ASTREA	M	A	M	A
Servicio SIFA	A	MA	MA	A
Servicio SIJA	A	MA	MA	A
Servicio ATENEA	A	MA	MA	M
Servicio SyMResa	M	A	A	A
Servicio SIGIE	A	A	A	A
Servicio SITT	A	A	A	A
Servicio DIPS	A	A	A	A
Servicio gestión documental (Orfeo)	MA	A	A	A
Servicio KACTUS	A	A	MA	A
Servicio SICON	A	A	A	MA
Servicio de correo electrónico	A	A	A	M
Servicio ISOLUCION	M	M	M	A
Servicio Página Web	MB	A	A	A
Servicio Intranet	M	A	M	M
Servicio SyM Infraestructura	M	A	A	B
Servicio PCT	M	A	A	M
Servicio SID	B	A	A	B
Servicio SIAP	B	A	A	A
Servicio SIOPSR	M	A	A	B
Servicio de Viáticos	M	A	A	M
Servicio ULISES	M	A	A	M
Servicio SOLSIREH	A	M	M	B
Servicio Atlas Interactivo	MB	A	A	M
Servicio Registros Administrativos	MB	M	M	B
Servicio HelpDesk (Dexon)	B	B	B	B
Servicio Consulta de Imágenes	MB	MB	MB	MB
[SW] Software				
Software SIBAS	A	A	A	A
Software ASTREA	M	A	M	A
Software SIFA	A	MA	MA	A
Software SIJA	A	MA	MA	A
Software ATENEA	A	MA	MA	M
Software SyMResa	M	A	A	A
Software SIGIE	A	A	A	A
Software SITT	A	A	A	A
Software DIPS	A	A	A	A
Software gestión documental (Orfeo)	MA	A	A	A
Software KACTUS	A	A	MA	A

Tabla 4. (Continuación)

Tipo / Nombre del Activo	Dimensiones			
	[C]	[I]	[A]	[D]
Software SICON	A	A	A	MA
Software de correo electrónico	A	A	A	M
Software ISOLUCION	M	M	M	A
Software Página Web	MB	A	A	A
Software Intranet	M	A	M	M
Software SyM Infraestructura	M	A	A	B
Software PCT	M	A	A	M
Software SID	B	A	A	B
Software SIAP	B	A	A	A
Software SIOPSR	M	A	A	B
Software Viáticos	M	A	A	M
Software ULISES	M	A	A	M
Software SOLSIREH	A	M	M	B
Sistema Atlas Interactivo	MB	A	A	M
Software Registros Administrativos	MB	M	M	B
Software HelpDesk (Dexon)	B	B	B	B
Sistema Consulta de Imágenes Docuware	MB	MB	MB	MB
[Hw] Hardware				
Servidor web SIBAS	A	A	A	A
Servidor BLADE (DB SIBAS)	A	A	A	A
Servidor web ASTREA	M	A	M	A
Servidor BLADE (DB ASTREA)	M	A	M	A
Servidor web PUBLICACION DE CONTENIDOS SIFA	A	MA	MA	A
Servidor BLADE (PUBLICACION DE CONTENIDOS SIJA)	A	MA	MA	A
Servidor BLADE (DB SIJA)	A	MA	MA	A
Servidor BLADE (PUBLICACION DE CONTENIDOS ATENEA)	A	MA	MA	M
Servidor BLADE (DB ATENEA)	A	MA	MA	M
Servidor web SyMResa	M	A	A	A
Servidor BLADE (DB SyMResa)	M	A	A	A
Servidor web SIGIE	A	A	A	A
Servidor DB SIGIE	A	A	A	A
Servidor web SITT	A	A	A	A
Servidor DB SITT	A	A	A	A
Servidor web DIPS	A	A	A	A
Servidor DB DIPS	A	A	A	A
Servidor gestión documental (Orfeo)	MA	A	A	A
Servidor KACTUS	A	A	MA	A
Servidor DB KACTUS	A	A	MA	A

Tabla 4. (Continuación)

Tipo / Nombre del Activo	Dimensiones			
	[C]	[I]	[A]	[D]
Servidor SICON	A	A	A	MA
Servidor DB SICON	A	A	A	MA
Servidor DB correo electrónico	A	A	A	M
Servidor Web WebAccess	A	A	A	M
Servidor correo electrónico	A	A	A	M
Firewall (perimetral/interno)	A	A	A	A
Servidor web ISOLUCION	M	M	M	A
Servidor BLADE (DB ISOLUCION)	M	M	M	A
Servidor Página Web	MB	A	A	A
Servidor BLADE (DB Página Web)	MB	A	A	A
Servidor Intranet	M	A	M	M
Servidor BLADE (DB Intranet)	M	A	M	M
Servidor web SyM Infraestructura	M	A	A	B
Servidor BLADE (DB SyM Infraestructura)	M	A	A	B
Servidor PCT	M	A	A	M
Servidor DB PCT	M	A	A	M
Servidor SID	B	A	A	B
Servidor DB SID	B	A	A	B
Servidor SIAP	B	A	A	A
Servidor web SIOPSR	M	A	A	B
Servidor BLADE (DB SIOPSR)	M	A	A	B
Servidor Viáticos	M	A	A	M
Servidor DB Viáticos	M	A	A	M
Servidor ULISES	M	A	A	M
Servidor DB ULISES	M	A	A	M
Servidor SOLSIREH	A	M	M	B
Server web Atlas Interactivo	MB	A	A	M
Server DB Atlas Interactivo	MB	A	A	M
Sistema de aire acondicionado	MB	A	A	A
Array EVA4000	MB	A	A	M
Array EVA6400	MB	A	A	M
Servidor controlador de domino	M	A	A	B
SwitchCatalyst 3750	MB	A	A	A
OpenScapeVoice	MB	A	A	M
Servidor BLADE (DB Registros Administrativos)	MB	M	M	B
Servidor web Help Desk (Dexon)	B	B	B	B
Sistema contra incendios	MB	A	A	B
Servidor web Sistema de Consulta de Imágenes	MB	MB	MB	MB
Servidor BLADE (DB Sistema de consulta de imágenes)	MB	MB	MB	MB

Tabla 4. (Continuación)

Tipo / Nombre del Activo	Dimensiones			
	[C]	[I]	[A]	[D]
[P] Personal				
Oficial de Seguridad Informática	M	A	A	B
Administrador de Infraestructura	M	A	MA	B
Administrador de Base de Datos	A	A	MA	B

Fuente: Autor

7.2 IDENTIFICACION Y VALORACIÓN DE AMENAZAS

7.2.1 Identificación de amenazas. De acuerdo con el catálogo establecido por Magerit, se presentan las posibles amenazas asociadas a cada uno de los activos y relacionadas con [N] Desastres naturales, [I] De origen industrial, [E] Errores y fallos no intencionados y, [A] Ataques intencionados:

Tabla 5. Identificación de amenazas

Tipo Activo / Nombre Activo / Amenaza asociada
[I] Datos / Información
Información SIBAS
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información ASTREA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SIFA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SIJA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información ATENEA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SyMResa
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SIGIE
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SITT
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información DIPS
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información gestión documental (Orfeo)

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información KACTUS
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SICON
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información correo electrónico
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información ISOLUCION
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información Página Web
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información Intranet
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SyM Infraestructura
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SyM Paz y Desarrollo
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información PCT
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SID
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SIAP

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SIOPSR
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información Viáticos
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información ULISES
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información SOLSIREH
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información Atlas Interactivo
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información Registros Administrativos
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
Información Sistema de Consulta de Imágenes
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[S] servicios
Servicio SIBAS
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio ASTREA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SIFA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SIJA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servicio ATENEA
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SyMResa
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SIGIE
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SITT
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio DIPS
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio gestión documental (Orfeo)
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio KACTUS
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SICON
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio de correo electrónico
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio ISOLUCION
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio Página Web
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servicio Intranet
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SyM Infraestructura
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio PCT
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SID
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SIAP
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SIOPSR
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio de Viáticos
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio ULISES
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio SOLSIREH
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio Atlas Interactivo
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio Registros Administrativos
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servicio HelpDesk (Dexon)
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
Servicio Consulta de Imágenes
[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.9] Errores de [re-] encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caídas del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.9] [Re-] encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.13] Repudio
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.24] Denegación de servicio
[SW] Software
Software SIBAS
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software ASTREA
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SIFA
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SIJA
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software ATENEA
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SyMResa
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SIGIE
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SITT
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software DIPS
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software gestión documental (Orfeo)
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software KACTUS
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SICON
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software de correo electrónico
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software ISOLUCION
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software Página Web
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software Intranet
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SyM Infraestructura
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software PCT
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SID
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.22] Manipulación de programas
Software SIAP
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SIOPSR
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software Viáticos

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software ULISES
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software SOLSIREH
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Sistema Atlas Interactivo
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software Registros Administrativos
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Software HelpDesk (Dexon)
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
Sistema Consulta de Imágenes Docuware
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas
[E.21] Errores de mantenimiento / actualización de programas
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[Hw] Hardware
Servidor web SIBAS
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servidor BLADE (DB SIBAS)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web ASTREA
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB ASTREA)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web PUBLICACION DE CONTENIDOS SIFA
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (PUBLICACION DE CONTENIDOS SIJA)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB SIJA)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (PUBLICACION DE CONTENIDOS ATENEA)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB ATENEA)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web SyMResa
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB SyMResa)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web SIGIE
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servidor DB SIGIE
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web SITT
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB SITT
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web DIPS
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB DIPS
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor gestión documental (Orfeo)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor KACTUS
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB KACTUS
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor SICON
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB SICON
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB correo electrónico
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servidor Web WebAccess
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor correo electrónico
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Firewall (perimetral/interno)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web ISOLUCION
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB ISOLUCION)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor Página Web
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB Página Web)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor Intranet
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB Intranet)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web SyM Infraestructura
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB SyM Infraestructura)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servidor PCT
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB PCT
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor SID
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB SID
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor SIAP
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web SIOPSR
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB SIOPSR)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor Viáticos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB Viáticos
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor ULISES
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor DB ULISES
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Servidor SOLSIREH
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Server web Atlas Interactivo
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Server DB Atlas Interactivo
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Sistema de aire acondicionado
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Array EVA4000
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Array EVA6400
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor controlador de domino
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
SwitchCatalyst 3750
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
OpenScapeVoice
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB Registros Administrativos)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web Help Desk (Dexon)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Sistema contra incendios
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor web Sistema de Consulta de Imágenes
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
Servidor BLADE (DB Sistema de consulta de imágenes)
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres naturales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte de suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (Hw)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[P] Personal
Oficial de Seguridad Informática
[E.7] Deficiencias en la organización
[E.19] Fugas de información
[E.28] Indisponibilidad del personal
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social
Administrador de Infraestructura
[E.7] Deficiencias en la organización
[E.19] Fugas de información
[E.28] Indisponibilidad del personal
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

Tabla 5. (Continuación)

Tipo Activo / Nombre Activo / Amenaza asociada
Administrador de Base de Datos
[E.7] Deficiencias en la organización
[E.19] Fugas de información
[E.28] Indisponibilidad del personal
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

Fuente: Autor

7.2.2 Valoración de amenazas. Del anterior listado de activos y amenazas, se toman aquellos asociados con las bases de datos de la Entidad (activos tipo Información), las cuales serán valoradas en los sentidos de degradación y probabilidad:

Degradación: Cuán perjudicado resultaría el activo en cada dimensión de seguridad:

[C] Confidencialidad: Importancia de que los datos fueran conocidos por personas no autorizadas.
[I] Integridad: Importancia de que los datos fueran modificados sin control.
[A] Autenticidad: Importancia de que quien accede a los datos no sea quien realmente se cree.
[D] Disponibilidad: Importancia de que los datos no estuviesen disponibles.

Se considera una escala porcentual para representar el impacto en los activos por cada dimensión:

Tabla 6. Escala porcentual para valorar dimensiones de seguridad

Impacto	Valor cuantitativo	Valor
Muy alto	100%	5
Alto	75%	4
Medio	50%	3
Bajo	20%	2
Muy bajo	5%	1

Fuente: Lorena Suarez Sierra. (2013). Sistema de Gestión de la Seguridad de la Información - SGSI

Probabilidad: Cuán probable es que se materialice la amenaza en escala numérica como frecuencia de ocurrencia:

Tabla 7. Escala numérica frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

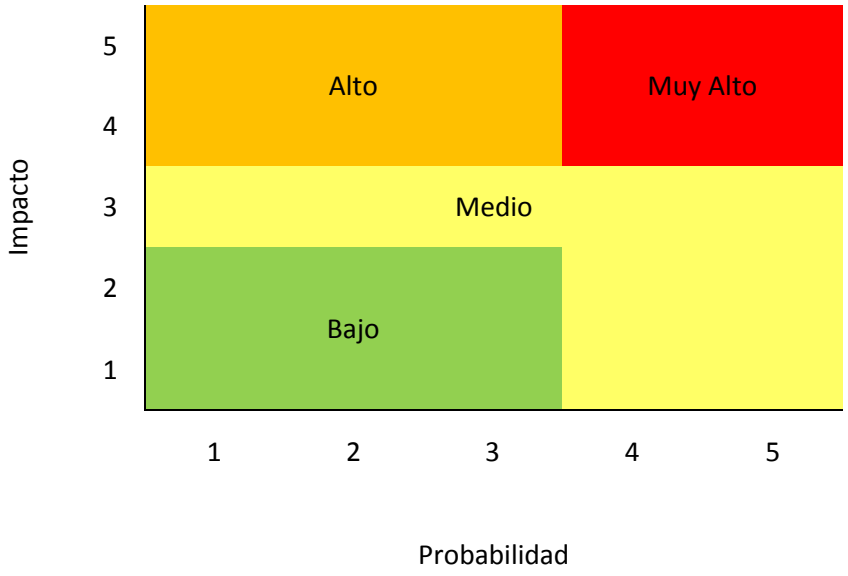
Fuente: Lorena Suarez Sierra. (2013). Sistema de Gestión de la Seguridad de la Información – SGSI

Valoración impacto potencial: Medida del daño sobre el activo al materializarse una amenaza. Se calcula utilizando las escalas numéricas tanto de la valoración de activos por cada dimensión y la degradación por cada dimensión en cada amenaza.

Valoración riego potencial: Medida del daño probable sobre un sistema. Se calcula con el impacto por dimensión y la probabilidad de ocurrencia (frecuencia de la amenaza).

La escala numérica definida para establecer la importancia del riesgo es:

Figura 1. Escala valoración del riesgo



Fuente: Autor

Aclaradas las mediciones utilizadas en el proceso de valoración de impacto y riesgo, se presenta el resultado por cada activo y amenaza:

Tabla 8.Valoración Impacto y Riesgo

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
Información SIBAS									
[E.1] Errores de los usuarios	3	2	3		2	Bajo	Medio		Bajo
[E.2] Errores de administrador	3	2	3		2	Bajo	Medio		Bajo
[E.15] Alteración accidental de la información	3		3				Medio		
[E.18] Destrucción de información	1				2				Bajo
[E.19] Fugas de información	3	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	3	2		Bajo	Medio	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	3		2	Bajo	Medio		Bajo
[A.11] Acceso no autorizado	1	2	3			Bajo	Medio		
[A.15] Modificación deliberada de la información	3		3				Medio		
[A.18] Destrucción de información	2				2				Bajo
[A.19] Divulgación de información	3	2				Bajo			
Información ASTREA									
[E.1] Errores de los usuarios	4	2	3		2	Medio	Medio		Medio
[E.2] Errores de administrador	4	2	3		3	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		3				Medio		
[E.18] Destrucción de información	2				2				Bajo
[E.19] Fugas de información	1	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	3	2		Bajo	Medio	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	3		2	Bajo	Medio		Bajo
[A.11] Acceso no autorizado	1	2	3			Bajo	Medio		
[A.15] Modificación deliberada de la información	2		3				Medio		
[A.18] Destrucción de información	1				2				Bajo
[A.19] Divulgación de información	2	2				Bajo			
Información SIFA									
[E.1] Errores de los usuarios	3	2	5		3	Bajo	Alto		Medio
[E.2] Errores de administrador	4	2	4		3	Medio	Muy Alto		Medio
[E.15] Alteración accidental de la información	3		5				Alto		
[E.18] Destrucción de información	3				3				Medio
[E.19] Fugas de información	4	3				Medio			
[A.5] Suplantación de la identidad del usuario	1	4	5	5		Alto	Alto	Alto	
[A.6] Abuso de privilegios de acceso	1	4	5		3	Alto	Alto		Medio
[A.11] Acceso no autorizado	1	4	5			Alto	Alto		
[A.15] Modificación deliberada de la información	3		5				Alto		
[A.18] Destrucción de información	1				3				Medio
[A.19] Divulgación de información	4	4				Muy Alto			
Información SIJA									
[E.1] Errores de los usuarios	3	2	4		2	Bajo	Alto		Bajo
[E.2] Errores de administrador	4	1	3		1	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		4				Alto		

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
[E.18] Destrucción de información	2				2				Bajo
[E.19] Fugas de información	2	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	3	4	4		Medio	Alto	Alto	
[A.6] Abuso de privilegios de acceso	1	3	4		2	Medio	Alto		Bajo
[A.11] Acceso no autorizado	1	3	4			Medio	Alto		
[A.15] Modificación deliberada de la información	2		4				Alto		
[A.18] Destrucción de información	2				2				Bajo
[A.19] Divulgación de información	2	3				Medio			
Información ATENEA									
[E.1] Errores de los usuarios	3	2	2		2	Bajo	Bajo		Bajo
[E.2] Errores de administrador	4	1	3		1	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		2				Bajo		
[E.18] Destrucción de información	2				2				Bajo
[E.19] Fugas de información	2	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	3	2	2		Medio	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	3	2		2	Medio	Bajo		Bajo
[A.11] Acceso no autorizado	1	3	2			Medio	Bajo		
[A.15] Modificación deliberada de la información	2		2				Bajo		
[A.18] Destrucción de información	2				2				Bajo
[A.19] Divulgación de información	2	3				Medio			
Información SyMResa									
[E.1] Errores de los usuarios	1	1	1		1	Bajo	Bajo		Bajo
[E.2] Errores de administrador	2	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	2		2				Bajo		
[E.18] Destrucción de información	1				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	1	1	1		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	1	1		1	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	1	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	2		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	2				Bajo			
Información SIGIE									
[E.1] Errores de los usuarios	2	2	3		2	Bajo	Medio		Bajo
[E.2] Errores de administrador	3	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	2		3				Medio		
[E.18] Destrucción de información	1				2				Bajo
[E.19] Fugas de información	1	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	3	3	3		Medio	Medio	Medio	
[A.6] Abuso de privilegios de acceso	1	3	3		2	Medio	Medio		Bajo

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
[A.11] Acceso no autorizado	1	3	3			Medio	Medio		
[A.15] Modificación deliberada de la información	2		3				Medio		
[A.18] Destrucción de información	1				2				Bajo
[A.19] Divulgación de información	2	3				Medio			
Información SITT									
[E.1] Errores de los usuarios	3	2	3		2	Bajo	Medio		Bajo
[E.2] Errores de administrador	4	1	2		1	Medio	Medio		Medio
[E.15] Alteración accidental de la información	2		3				Medio		
[E.18] Destrucción de información	2				2				Bajo
[E.19] Fugas de información	3	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	3	3	2		Medio	Medio	Bajo	
[A.6] Abuso de privilegios de acceso	1	3	3		2	Medio	Medio		Bajo
[A.11] Acceso no autorizado	1	3	3			Medio	Medio		
[A.15] Modificación deliberada de la información	3		3				Medio		
[A.18] Destrucción de información	3				2				Bajo
[A.19] Divulgación de información	3	2				Bajo			
Información DIPS									
[E.1] Errores de los usuarios	1	2	3		2	Bajo	Medio		Bajo
[E.2] Errores de administrador	1	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		3				Medio		
[E.18] Destrucción de información	1				2				Bajo
[E.19] Fugas de información	1	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	3	3	3		Medio	Medio	Medio	
[A.6] Abuso de privilegios de acceso	1	3	3		2	Medio	Medio		Bajo
[A.11] Acceso no autorizado	1	3	3			Medio	Medio		
[A.15] Modificación deliberada de la información	1		3				Medio		
[A.18] Destrucción de información	1				2				Bajo
[A.19] Divulgación de información	1	2				Bajo			
Información gestión documental (Orfeo)									
[E.1] Errores de los usuarios	4	1	1		1	Medio	Medio		Medio
[E.2] Errores de administrador	4	1	2		1	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		2				Bajo		
[E.18] Destrucción de información	2				1				Bajo
[E.19] Fugas de información	2	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	1	1	1		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	1	1		1	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	1	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	2		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	2	1				Bajo			

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
Información KACTUS									
[E.1] Errores de los usuarios	4	2	4		3	Medio	Muy Alto		Medio
[E.2] Errores de administrador	4	2	3		3	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		3				Medio		
[E.18] Destrucción de información	2				3				Medio
[E.19] Fugas de información	2	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	4	4	5		Alto	Alto	Alto	
[A.6] Abuso de privilegios de acceso	1	4	4		3	Alto	Alto		Medio
[A.11] Acceso no autorizado	1	4	4			Alto	Alto		
[A.15] Modificación deliberada de la información	2		4				Alto		
[A.18] Destrucción de información	1				3				Medio
[A.19] Divulgación de información	3	4				Alto			
Información SICON									
[E.1] Errores de los usuarios	3	1	2		3	Bajo	Bajo		Medio
[E.2] Errores de administrador	2	1	3		1	Bajo	Medio		Bajo
[E.15] Alteración accidental de la información	2		3				Medio		
[E.18] Destrucción de información	2				3				Medio
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	2	2		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	2		3	Bajo	Bajo		Medio
[A.11] Acceso no autorizado	1	2	2			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		2				Bajo		
[A.18] Destrucción de información	1				3				Medio
[A.19] Divulgación de información	2	3				Medio			
Información correo electrónico									
[E.1] Errores de los usuarios	3	1	2		2	Bajo	Bajo		Bajo
[E.2] Errores de administrador	2	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		2				Bajo		
[E.18] Destrucción de información	1				2				Bajo
[E.19] Fugas de información	2	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	2	2		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	2		2	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	2	2			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		2				Bajo		
[A.18] Destrucción de información	1				2				Bajo
[A.19] Divulgación de información	2	2				Bajo			
Información ISOLUCION									
[E.1] Errores de los usuarios	2	1	1		1	Bajo	Bajo		Bajo
[E.2] Errores de administrador	3	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	3		2				Bajo		

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
[E.18] Destrucción de información	2				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	1	1	1		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	1	1		1	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	1	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	2		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	1				Bajo			
Información Página Web									
[E.1] Errores de los usuarios	3	1	2		3	Bajo	Bajo		Medio
[E.2] Errores de administrador	4	1	3		3	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		2				Bajo		
[E.18] Destrucción de información	3				3				Medio
[E.19] Fugas de información	4	1				Medio			
[A.5] Suplantación de la identidad del usuario	2	1	2	3		Bajo	Bajo	Medio	
[A.6] Abuso de privilegios de acceso	1	1	2		3	Bajo	Bajo		Medio
[A.11] Acceso no autorizado	1	1	2			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		2				Bajo		
[A.18] Destrucción de información	1				3				Medio
[A.19] Divulgación de información	2	1				Bajo			
Información Intranet									
[E.1] Errores de los usuarios	4	1	2		2	Medio	Medio		Medio
[E.2] Errores de administrador	4	1	3		3	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		2				Bajo		
[E.18] Destrucción de información	2				2				Bajo
[E.19] Fugas de información	2	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	2	2		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	2		2	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	2	2			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		2				Bajo		
[A.18] Destrucción de información	1				2				Bajo
[A.19] Divulgación de información	1	1				Bajo			
Información SyM Infraestructura									
[E.1] Errores de los usuarios	1	1	1		1	Bajo	Bajo		Bajo
[E.2] Errores de administrador	1	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		2				Bajo		
[E.18] Destrucción de información	1				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	1	2		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	1		1	Bajo	Bajo		Bajo

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
[A.11] Acceso no autorizado	1	2	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	2				Bajo			
Información SyM Paz y Desarrollo									
[E.1] Errores de los usuarios	1	1	1		1	Bajo	Bajo		Bajo
[E.2] Errores de administrador	1	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		2				Bajo		
[E.18] Destrucción de información	1				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	1	2		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	1		1	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	2	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	2				Bajo			
Información PCT									
[E.1] Errores de los usuarios	3	2	3		2	Bajo	Medio		Bajo
[E.2] Errores de administrador	3	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	4		3				Medio		
[E.18] Destrucción de información	2				2				Bajo
[E.19] Fugas de información	2	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	3	3	3		Medio	Medio	Medio	
[A.6] Abuso de privilegios de acceso	1	3	3		2	Medio	Medio		Bajo
[A.11] Acceso no autorizado	1	3	3			Medio	Medio		
[A.15] Modificación deliberada de la información	2		3				Medio		
[A.18] Destrucción de información	2				2				Bajo
[A.19] Divulgación de información	2	2				Bajo			
Información SID									
[E.1] Errores de los usuarios	1	1	3		1	Bajo	Medio		Bajo
[E.2] Errores de administrador	1	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		3				Medio		
[E.18] Destrucción de información	1				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	3	3		Bajo	Medio	Medio	
[A.6] Abuso de privilegios de acceso	1	2	3		1	Bajo	Medio		Bajo
[A.11] Acceso no autorizado	1	2	3			Bajo	Medio		
[A.15] Modificación deliberada de la información	1		3				Medio		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	1				Bajo			

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
Información SIAP									
[E.1] Errores de los usuarios	3	1	3		2	Bajo	Medio		Bajo
[E.2] Errores de administrador	2		2		1		Bajo		Bajo
[E.15] Alteración accidental de la información	1		3				Medio		
[E.18] Destrucción de información	1				2				Bajo
[E.19] Fugas de información	2								
[A.5] Suplantación de la identidad del usuario	1		3	3			Medio	Medio	
[A.6] Abuso de privilegios de acceso	1		3		2		Medio		Bajo
[A.11] Acceso no autorizado	1		3				Medio		
[A.15] Modificación deliberada de la información	2		3				Medio		
[A.18] Destrucción de información	2				2				Bajo
[A.19] Divulgación de información	2								
Información SIOPSR									
[E.1] Errores de los usuarios	1	1	1		1	Bajo	Bajo		Bajo
[E.2] Errores de administrador	1	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		2				Bajo		
[E.18] Destrucción de información	1				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	1	1	1		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	1	1		1	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	1	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	2				Bajo			
Información Viáticos									
[E.1] Errores de los usuarios	1	2	3		2	Bajo	Medio		Bajo
[E.2] Errores de administrador	1	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		2				Bajo		
[E.18] Destrucción de información	1				2				Bajo
[E.19] Fugas de información	1	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	3	3	3		Medio	Medio	Medio	
[A.6] Abuso de privilegios de acceso	1	3	3		2	Medio	Medio		Bajo
[A.11] Acceso no autorizado	1	3	3			Medio	Medio		
[A.15] Modificación deliberada de la información	1		3				Medio		
[A.18] Destrucción de información	1				2				Bajo
[A.19] Divulgación de información	1	3				Medio			
Información ULISES									
[E.1] Errores de los usuarios	4	2	3		3	Medio	Medio		Medio
[E.2] Errores de administrador	4	2	3		3	Medio	Medio		Medio
[E.15] Alteración accidental de la información	3		3				Medio		

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
[E.18] Destrucción de información	2				3				Medio
[E.19] Fugas de información	2	2				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	3	2		Bajo	Medio	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	3		3	Bajo	Medio		Medio
[A.11] Acceso no autorizado	1	2	3			Bajo	Medio		
[A.15] Modificación deliberada de la información	2		3				Medio		
[A.18] Destrucción de información	2				3				Medio
[A.19] Divulgación de información	2	3				Medio			
Información SOLSIREH									
[E.1] Errores de los usuarios	1	1	1		1	Bajo	Bajo		Bajo
[E.2] Errores de administrador	1	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	1		2				Bajo		
[E.18] Destrucción de información	1				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	2	1	1		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	2	1		1	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	2	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	2				Bajo			
Información Atlas Interactivo									
[E.1] Errores de los usuarios	2	1	2		2	Bajo	Bajo		Bajo
[E.2] Errores de administrador	3	1	2		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	2		2				Bajo		
[E.18] Destrucción de información	1				2				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	1	1	1		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	1	1		2	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	1	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		2				Bajo		
[A.18] Destrucción de información	1				2				Bajo
[A.19] Divulgación de información	1	1				Bajo			
Información Registros Administrativos									
[E.1] Errores de los usuarios	4	1	3		2	Medio	Medio		Medio
[E.2] Errores de administrador	4	1	3		2	Medio	Medio		Medio
[E.15] Alteración accidental de la información	4		3				Medio		
[E.18] Destrucción de información	3				2				Bajo
[E.19] Fugas de información	4	1				Medio			
[A.5] Suplantación de la identidad del usuario	2	1	3	5		Bajo	Medio	Alto	
[A.6] Abuso de privilegios de acceso	2	1	3		2	Bajo	Medio		Bajo

Tabla 8. (Continuación)

Activo / Amenaza	Frecuencia de la amenaza	Valoración Impacto potencial				Valoración Riesgo potencial			
		[C]	[I]	[A]	[D]	[C]	[I]	[A]	[D]
[A.11] Acceso no autorizado	2	1	3			Bajo	Medio		
[A.15] Modificación deliberada de la información	3		3				Medio		
[A.18] Destrucción de información	3				2				Bajo
[A.19] Divulgación de información	4	1				Medio			
Información Sistema de Consulta de Imágenes									
[E.1] Errores de los usuarios	2	1	1		1	Bajo	Bajo		Bajo
[E.2] Errores de administrador	3	1	1		1	Bajo	Bajo		Bajo
[E.15] Alteración accidental de la información	2		1				Bajo		
[E.18] Destrucción de información	1				1				Bajo
[E.19] Fugas de información	1	1				Bajo			
[A.5] Suplantación de la identidad del usuario	1	1	1	1		Bajo	Bajo	Bajo	
[A.6] Abuso de privilegios de acceso	1	1	1		1	Bajo	Bajo		Bajo
[A.11] Acceso no autorizado	1	1	1			Bajo	Bajo		
[A.15] Modificación deliberada de la información	1		1				Bajo		
[A.18] Destrucción de información	1				1				Bajo
[A.19] Divulgación de información	1	1				Bajo			

Fuente: Autor

7.3 SALVAGUARDIAS

Con la valoración del Riesgo Potencial, se toman aquellas amenazas de Alta y Muy Alta criticidad con el fin de realizar la respectiva verificación de controles que en este momento la Entidad tiene implementados para determinar su efectividad.

Se identifican por cada amenaza que podría afectar las bases de datos, los controles existentes en la Entidad con el fin de disminuir los riesgos a los que están expuestos los activos:

[E.1] Errores de los usuarios / [E.2] Errores de administrador / [E.15] Alteración accidental de la información:

11.4.1 Políticas para el uso de los servicios de red de datos
11.4.2 Autenticación de usuarios para conexiones externas
11.4.3 Identificación de equipos en la red
11.4.4 Diagnóstico remoto y protección de la configuración de puertos
11.4.5 Separación en la redes
11.4.6 Control de conexión a la red de trabajo

11.4.7 Control de enrutamiento de red
10.6.1 Controles de red
10.6.2 Seguridad de los servicios de red
10.7.1 Gestión de medios removibles
10.7.2 Gestión de destrucción de medios
11.6.1 Restricción de acceso a los sistemas de información
11.6.2 Aislamiento de sistemas sensibles
11.5.1 Procedimientos para inicio de sesión de las estaciones de trabajo
11.5.2 Identificación y autenticación de los usuarios
11.5.3 Sistema de gestión de contraseñas
11.5.5 Tiempo de la inactividad de la sesión
11.5.6 Limitación en los periodos de tiempo de conexión a servicios y aplicaciones
10.1.4 Separación de los ambientes de Desarrollo, prueba y producción
11.2.4 Revisión de los permisos asignados a los usuarios
11.1.1 Política de Control de Acceso
11.2.1 Registro de Usuarios
11.2.2 Gestión de privilegios
11.2.3 Gestión de Contraseñas
11.3.1 Uso de las contraseñas
7.1.1 Inventario de activos tecnológicos y de la información
7.1.2 Responsables de los activos tecnológicos
7.1.3 Uso aceptable de los activos tecnológicos
10.7.1 Gestión de medios removibles
10.7.2 Destrucción de medios
10.8.3 Medios físicos en transito

[E.18] Destrucción de información

10.5.1 Respaldo de la información
8.3.2 Devolución de activos tecnológicos
9.2.6 Eliminación, destrucción y reutilización de equipos
10.7.2 Destrucción de medios
10.7.1 Gestión de medios removibles
10.8.3 Medios físicos en transito
10.10.2 Monitoreo del uso del sistema
11.7.2 Teletrabajo / trabajo remoto

[E.19] Fugas de información

10.8.1 Políticas y procedimientos del intercambio de información
10.8.2 Acuerdos para el intercambio de información
10.8.4 Mensajería Electrónica
10.5.1 Respaldo de la información
10.7.1 Gestión de medios removibles
10.7.4 Seguridad de la documentación de los sistemas de intercambio de información
10.9.3 Información pública /disponible al público
7.2.1 Normas para clasificación de la información
7.2.2 Identificación y Manejo de la información

[A.5] Suplantación de la identidad del usuario / [A.6] Abuso de privilegios de acceso / [A.11] Acceso no autorizado

9.2.3 Seguridad en el cableado
10.6.1 Controles de la red
10.6.2 Seguridad de los servicios de red
10.8.4 Mensajería electrónica
11.4.5 Separación en redes
11.4.6 Control de conexión a la red de trabajo
11.4.7 Control de enrutamiento de red
10.4.1 Controles contra código malicioso
10.4.2 Controles contra código móvil
9.1.2 Controles físicos de entrada
9.1.3 Aseguramiento de oficinas, cuartos e instalaciones
9.1.6 Acceso público, envíos y áreas de carga

[A.15] Modificación deliberada de la información / [A.18] Destrucción de información / [A.19] Divulgación de información

15.3.1 Controles para auditoría del sistema
15.3.2 Protección de las herramientas para auditoría del sistema
10.10.1 Registros de auditoría
10.10.2 Monitoreo del uso del sistema
10.10.3 Protección de registros de monitoreo
10.10.4 Registros de monitoreo de administradores y operadores
10.10.5 Registro de fallas
10.10.6 Sincronización de relojes

De acuerdo a la valoración del riesgo (Alto y Muy Alto), resultado del análisis de riesgos realizado en el Centro de Datos de la Entidad; los riesgos que deben ser tratados son los siguientes:

[E.1] Errores de los usuarios
[E.2] Errores de administrador
[E.15] Alteración accidental de la información
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.19] Divulgación de información

8. PLAN DE AUDITORÍA

El estándar ISO 27001 es aplicado a nivel internacional para la administración de Seguridad de la Información ya que aplica para todo tipo de actividad y tamaño de la empresa, además que su propósito es brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). (NTC-ISO-IEC 27001).

Si bien hablamos de Seguridad de la Información, el tema de estudio hace parte fundamental de la implementación del Sistema de Gestión que adelanta la Entidad en este momento, por lo tanto el plan de auditoría se basa en la norma ISO 27001 que establece directrices para la auditoria en los sistemas de gestión de calidad o ambiental, pero se adapta su aplicación a la auditoría en seguridad informática en bases de datos de la Entidad caso de estudio.

Tabla 9. Plan de auditoría

CONCEPTO	DETALLES	
Objeto de la auditoría	La auditoría a realizar tiene por objeto determinar el grado de conformidad en las bases de datos existentes en el Centro de Datos del Departamento para la Prosperidad Social - DPS, con respecto a la norma NTC-ISO/IEC 27001:2013	
Alcance de la auditoría	La evaluación a llevar a cabo por el equipo auditor se referirá a las condiciones de acceso y administración del Centro de Datos y bases de datos respectivamente, afectando al grupo de Infraestructura y Soporte de Tecnologías de la Información del Departamento para la Prosperidad Social - DPS, sede principal	
Equipo auditor	Claudia Andrea Lasso	
Criterio de auditoría	NTC-ISO/IEC 27001:2013. Sistemas de Gestión de la Seguridad dela Información NTC-ISO/IEC 27002:2007. Código de práctica para la gestión de la seguridad de la Información	
Otra información necesaria	• Manual de Gestión Integral • Listado de Manuales, Guías y Procedimientos de uso interno y los publicados	
Representantes de auditado	Área / Proceso	Infraestructura y Soporte de Tecnologías de la Información
	Nombre y Apellidos	Giovanny Poveda

Tabla 9. (Continuación)

CONCEPTO	DETALLES	
Calendario de auditoría y horarios	Día / Hora	01/06/2015 - 10:00 - 12:00 02/06/2015 - 14:00 - 15:00 04/06/2015 - 11:00 - 12:00 05/06/2015 - 10:00 - 12:00
Idioma de la auditoría	Español	
Lista de distribución del informe de auditoría	Se elaborará un informe de la auditoria y se entregará a la Coordinación del área auditada en un plazo no superior a una semana desde su finalización.	

Fuente: Autor

9. DESARROLLO DE LA AUDITORÍA

Identificados los riesgos Alto y Muy altos, considerados en este proyecto como los que deben ser tratados con urgencia, así como los salvaguardias aplicados en la Entidad, es necesario establecer su existencia o no y cumplimiento de acuerdo a la norma ISO 27002, adicionalmente a una descripción sobre la verificación de cada control por cada base de datos, los cuales fueron estandarizados ya que aplican para mantener o mejorar la seguridad de todas las bases de datos:

Tabla 10. Verificación de controles

CONTROLES	EXISTE		CUMPLE		OBSERVACIÓN
	SI	NO	SI	NO	
GESTIÓN DE ACTIVOS					
RESPONSABILIDAD POR LOS ACTIVOS					
7.1.1 Inventario de activos tecnológicos y de la información	X		X		Es necesario establecer el procedimiento para la actualización del inventario actual
7.1.2 Responsables de los activos tecnológicos	X		X		La actualización es necesaria ya que responsables de Activos ya no labora en la Entidad
7.1.3 Uso aceptable de las activos tecnológicos	X			X	Se incluye en el Manual de Políticas el uso correcto del correo electrónico, de Internet y de dispositivos móviles. La Política se encuentra en proceso de aprobación por parte del Comité de Tecnología
SEGURIDAD FÍSICA Y DEL ENTORNO					
ÁREAS SEGURAS					
9.1.2 Controles físicos de entrada	X		X		El ingreso al área de Infraestructura se controla mediante tarjeta electrónica. El centro de datos tiene un sistema de tarjeta electrónica y clave, así como el diligenciamiento de una planilla de entrada-salida
9.1.3 Aseguramiento de oficinas, cuartos e instalaciones	X		X		Se cuenta con un esquema de vigilancia que restringe el acceso desde la recepción
9.1.6 Acceso público, envíos y áreas de carga	X		X		El esquema de vigilancia abarca ingreso principal y parqueaderos
SEGURIDAD DE LOS EQUIPOS					
9.2.3 Seguridad en el cableado	X			X	El cableado se encuentra protegido por canaletas y separados los de voz, datos y electricidad, debidamente rotulados. No se cuenta con planos de cableado estructurado debidamente actualizados ya que se han realizado durante el último año muchas modificaciones en las áreas

Tabla 10. (Continuación)

CONTROLES	EXISTE		CUMPLE		OBSERVACIÓN
	SI	NO	SI	NO	
GESTIÓN DE COMUNICACIONES Y OPERACIONES					
PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES					
10.1.4 Separación de los ambientes de Desarrollo, prueba y producción		X		X	Actualmente solo se cuenta con ambiente de pruebas y producción y se está adelantando un proceso de separación de éstos ambientes
PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS Y MÓVILES					
10.4.1 Controles contra código malicioso	X		X		Se cuenta con antivirus y medidas de control para su detección
10.4.2 Controles contra código móvil	X		X		El paquete de antivirus contiene las medidas de restricción necesarias tanto para los usuarios como en los reportes de eventos, los cuales son generados periódicamente
GESTIÓN DE LA SEGURIDAD DE LAS REDES					
10.6.1 Controles de la red	X		X		Está definido el esquema perimetral con la administración del firewall a cargo de personal específico
10.6.2 Seguridad de los servicios de red	X		X		quien determina la aplicación de políticas de protección como los filtros de contenido y demás sugeridas por el oficial de seguridad
MANEJO DE LOS MEDIOS					
10.7.1 Gestión de medios removibles	X			X	El documento de políticas es claro en este punto y relaciona el instructivo de borrado seguro de la información que en la práctica se aplica y la guía de clasificación y etiquetado de la información. Se ha masificado el uso de unidades externas de almacenamiento sin controles de uso; por tal razón se está implementando la restricción de puertos USB
10.7.2 Gestión de destrucción de medios	X			X	El único procedimiento claro es el borrado seguro de los equipos reutilizados, pero la destrucción apropiada no se encuentra implementada y no hay procedimientos asociados.
INTERCAMBIO DE LA INFORMACIÓN					
10.8.3 Medios físicos en transito	X		X		Se cuenta con servicio de mensajería y la información enviada por correspondencia se encriptan como buena práctica de seguridad, adicionalmente se cuenta con u n contrato de custodia de medios que garantiza la seguridad de las cintas que salen de la Entidad con los backup de información
10.8.4 Mensajería electrónica	X			X	La seguridad se configura con las aplicaciones del antivirus y firewall, internamente se configura el anti spam y aunque se cuenta con una herramienta de mensajería instantánea, los usuarios con privilegios pueden instalar otras herramientas no adecuadas
MONITOREO					
10.10.1 Registros de auditoría		X		X	
10.10.2 Monitoreo del uso del sistema		X		X	Se está investigando la implementación de una solución opensource que permita monitorear y centralizar todas estas acciones. Adicionalmente se debe validar el alcance del monitoreo. Actualmente no es posible hacer seguimiento a un incidente
10.10.3 Protección de registros de monitoreo		X		X	
10.10.4 Registros de monitoreo de administradores y operadores		X		X	
10.10.5 Registro de fallas		X		X	
10.10.6 Sincronización de relojes	X			X	El control existe pero no hay un procedimiento definido para la verificación y corrección de variaciones

Tabla 10. (Continuación)

CONTROLES	EXISTE		CUMPLE		OBSERVACIÓN
	SI	NO	SI	NO	
CONTROL DE ACCESO					
REQUISITOS DEL NEGOCIO PARA EL CONTROL DEL ACCESO					
11.1.1 Política de Control de Acceso	X		X		La política existe pero está en proceso de autorización. Aun así se cumple en la operatividad del área
GESTIÓN DEL ACCESO DE USUARIOS					
11.2.1 Registro de Usuarios	X		X		Existe el procedimiento para solicitud de creación y cancelación de cuentas de usuario; así como el Acuerdo Individual de Confidencialidad de información que cada funcionario diligencia al momento de su ingreso
11.2.2 Gestión de privilegios	X		X		Existe la política de control de acceso, así como los procedimientos internos para la asignación de privilegios de acuerdo al rol de los usuarios
11.2.3 Gestión de Contraseñas	X		X		Tanto la política como el Acuerdo Individual mencionan las pautas para la adecuada gestión de contraseñas
11.2.4 Revisión de los permisos asignados a los usuarios	X		X		Se tienen falencias en cuanto al ingreso de contratistas o cambios entre oficinas de los funcionarios ya que el área de Infraestructura no es informada sobre éstas novedades, dificultando la verificación de privilegios, la cual se hace inmediatamente al momento en que Talento Humano reporte las novedades de ingreso o retiro de funcionarios
RESPONSABILIDADES DE LOS USUARIOS					
11.3.1 Uso de las contraseñas	X			X	Se realizan campañas de concientización, se aplican niveles de seguridad como tiempo de caducidad, existe una política de gestión de contraseñas, pero se detecta un nivel medio de confidencialidad y complejidad entre los funcionarios al momento de usar sus contraseñas
CONTROL DEL ACCESO A LAS REDES					
11.4.1 Políticas para el uso de los servicios de red de datos	X			X	La política es clara, los controles de acceso existen y son aplicadas pero no se tiene control de los equipos portátiles que cada oficina cuenta como dotación adicional, los cuales pueden tener acceso a la red sin validación de usuario
11.4.2 Autenticación de usuarios para conexiones externas	X		X		La Entidad se encuentra desarrollando procesos de interoperabilidad a través de FTP, pero en el momento son los externos quienes proveen ese servicio al DPS mediante una VPN, a la cual no se puede acceder sin la autorización previa del área de Infraestructura
11.4.3 Identificación de equipos en la red	X			X	Si bien en un gran porcentaje el nombre del equipo establece el área al cual pertenece, esté no está asociado a su autenticación
11.4.4 Diagnóstico remoto y protección de la configuración de puertos	X			X	Se están documentando guías de aseguramiento para configuraciones estándar. Tantas guías como componentes de la red existan. Actualmente se encuentra en revisión por la de Servidores Win8 para asegurar la configuración del equipos a los requerimientos
11.4.5 Separación en la redes	X		X		Existe segmentación de red por cada programa y servidores
11.4.6 Control de conexión a la red de trabajo	X			X	El alcance de las políticas incluye en el caso del DPS todas las sedes a nivel nacional, así como las políticas de seguridad aplicadas al nivel central, pero se debería hacer un análisis de riesgos en éstos casos ya que las condiciones de accesibilidad no son las mismas en todas las regiones del país
11.4.7 Control de enrutamiento de red	X			X	

Tabla 10. (Continuación)

CONTROLES	EXISTE		CUMPLE		OBSERVACIÓN
	SI	NO	SI	NO	
CONTROL DEL ACCESO AL SISTEMA OPERATIVO					
11.5.1 Procedimientos para inicio de sesión de las estaciones de trabajo	X		X		El procedimiento de acceso valida el directorio activo, pero se requiere reforzar el buen uso y la generación de contraseñas y fortalecer la autenticación asociado al nombre del equipo
11.5.2 Identificación y autenticación de los usuarios	X		X		Se cuenta con nombres de usuario únicos y validación por directorio activo
11.5.3 Sistema de gestión de contraseñas	X		X		Reforzar la concientización en la importancia del uso de contraseñas seguras
11.5.5 Tiempo de la inactividad de la sesión	X			X	El tiempo programado de inactivación de sesión es prolongado y se deben fomentar las campañas de concientización para mantener seguro el inicio de sesión cuando los funcionarios no se encuentran en su sitio de trabajo
11.5.6 Limitación en los periodos de tiempo de conexión a servicios y aplicaciones	X			X	No se limitan los tiempos de conexión a los horarios laborales
CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN					
11.6.1 Restricción de acceso a los sistemas de información	X		X		Los módulos de administración y gestión de usuarios en los sistemas de información contemplan estas restricciones
11.6.2 Aislamiento de sistemas sensibles		X		X	No existe
CUMPLIMIENTO					
CONSIDERACIONES DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN					
15.3.1 Controles para auditoría del sistema	X			X	Existe una guía de desarrollo de software que incluye la auditoría dentro de los lineamientos de administración del sistema, pero no se realiza un seguimiento exhaustivo de la auditoría
15.3.2 Protección de las herramientas para auditoría del sistema	X		X		La información de auditoria se guarda en tablas vinculadas al sistema de información

Fuente: Autor

10. ANÁLISIS DE RESULTADOS

Tabla 11. Consolidado de verificación

CONTROLES	EXISTE		CUMPLE	
	SI	NO	SI	NO
Gestión de activos	3		2	1
Seguridad física y del entorno	4		3	1
Gestión de comunicaciones y operaciones	9	6	5	10
Control de acceso	19	1	11	10
Cumplimiento	2		1	1
TOTAL	37	7	22	23

Fuente: Autor

Como controles adicionales para fortalecer la seguridad en las bases de datos, se recomiendan:

Incrementar los controles de acceso a los sistemas de información mediante el uso de aplicaciones que verifiquen la fortaleza de las contraseñas, ayuden a determinar las políticas de renovación adecuadas o proporcionen un sistema de administración de tal manera que se pueda trabajar con contraseñas con un alto grado de complejidad sin necesidad de tener que recordarlas evitando así el uso de la misma contraseña para varias aplicaciones o accesos. Se pueden utilizar aplicaciones opensource como Jhon the Ripper y Keepass.

Fortalecer el control de auditoría para el acceso a redes y servicios relacionados, identificando métricas de usuarios registrados, aceptados y con revisión de accesos de acuerdo a los roles para todos los sistemas de información, de tal manera que se puedan establecer indicadores de seguimiento. Se recomiendan soluciones opensource como OpenNAC para la aplicación de políticas de accesos flexibles, administración de notificaciones, monitorización de usuarios en tiempo real y detección de sistemas operativos, firewall para hacer cumplir la política de acceso[4]

Implementar mediante desarrollo un gestor único de contraseñas que permita integrar todas las aplicaciones existentes en la Entidad y asociar las contraseñas al directorio activo, de tal forma que al reportar la novedad de retiro del usuario de la Entidad se inactiven automáticamente todos los servicios y accesos que tenía habilitados dicho usuario.

Configurar políticas de caducidad a las bases de datos Oracle, actualizando la asignación de contraseñas.

[4]Opensource NAC SOLUCION. Principales beneficios de OpenNac. Disponible en: http://www.opennac.org/opennac/en/about/why-opennac.html

Complementar el inventario de bases de datos funcionales y no funcionales a la gestión de capacidades para ajustar el uso de los recursos en pro del mejor rendimiento de los sistemas de información.

10.1 EVIDENCIAS DE AUDITORÍA

Durante el desarrollo de la auditoría se contaron con diversas herramientas para la recolección de información como son:

- Checklist de las condiciones de Seguridad en el Centro de Datos (Ver Anexo A)
- Cuestionario de la entrevista realizada sobre las condiciones de seguridad de las bases de datos (Ver Anexo B)
- Listado de procedimientos, guías, lineamientos o manuales existentes en el área de uso interno y publicados en la intranet:
    - Manual de políticas y lineamientos seguridad de la información (Ver Anexo C)
    - Política de Backup 2015 (Ver Anexo D)
    - Guía desarrollo de software(Ver Anexo E)
    - Planilla Control de backups2015 (Ver Anexo F)
    - Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario (Ver Anexo G)
    - Formato de Definición de Backups de Información (Ver Anexo H)
    - Formato de Registro de Backups Ejecutados (Ver Anexo I)
    - Formato Solicitud de Gestión de Cambios (Ver Anexo J)
    - Formato de Gestión de Incidentes DPS (Ver Anexo K)
    - Control de ingreso al centro de cómputo (Ver Anexo L)
    - Procedimiento de Creación y Cancelación de Cuentas de Usuario (Ver Anexo M)
    - Procedimiento de Ejecución de Backups (Ver Anexo N)
    - Procedimiento de Restauración de Backups (Ver Anexo O)
    - Procedimiento entrega bases de datos (Ver Anexo P)
    - Procedimiento de Gestión de Cambios (Ver Anexo Q)
    - Procedimiento de Implementación de Requerimientos en las BD (Ver Anexo R)
    - Procedimiento_Notificación_de_eventos_y_gestión_de_incidentes_de_seguridad v 1.2 (Ver Anexo S)
- Listado de procedimientos, gruías, lineamientos o manuales publicados en la intranet (Ver Anexo T)
    - Circular 02 de enero 19 de 2015, política de uso correo electrónico
    - Formato solicitud de creación y cancelación de cuentas de usuario
    - Acuerdo individual del manejo de información
    - Acuerdos de confidencialidad de información a terceros

- Acuerdo individual de confidencialidad de información

- Ejecución del comando netstat –abn para establecer los puertos a los que tienen acceso los equipos, identificando puertos permitidos en los equipos que tienen privilegios de administrador (Ver anexo U).

- Verificación de los nombres de equipos por áreas para la segmentación de la red, identificando no uniformidad en los nombres de equipos por área (Ver anexo V).

11. INFORME FINAL DE AUDITORÍA

Fecha del informe: Junio 5 de 2015

Nombre de la Entidad: Departamento para la Prosperidad Social – DPS

Objetivo: determinar el grado de conformidad en las bases de datos existentes en el Centro de Datos

Lugar de la Auditoría: Área de Infraestructura y Soporte de Tecnologías de la Información

Grupo de trabajo de Auditoría: Estudiante Especialización en Seguridad Informática Claudia Andrea Lasso

Fecha de inicio de la Auditoría: Junio 1 de 2015

Tiempo estimado del proceso de revisión: 6 horas

Fecha de finalización de la Auditoría: Junio 5 de 2015

Herramientas utilizadas:
Checklist para verificar los objetivos de control
Entrevistas y cuestionarios para el levantamiento de información
Trazas mediante documentación publicada o secuencia de comandos
Observación directa

Alcance: Controlar la existencia de las medidas necesarias para mantener la seguridad en las bases de datos

Procedimientos a aplicar:
Revisión de la política de seguridad de la información
Verificación de documentos, guías y procedimientos asociados a la política

Informe de las debilidades encontradas:

Tabla 12. Debilidades

SITUACIÓN ACTUAL	RECOMENDACIÓN	COMENTARIOS
Manual de políticas y lineamientos de seguridad de la información no publicada ni socializada	El Área de Infraestructura y Soporte de TI publicará y socializara el Manual de Políticas y lineamientos de seguridad de la información	De acuerdo
Inventario de activos desactualizado	El Área de Infraestructura y Soporte de TIdiseñará e implementará un procedimiento de actualización periódica de los activos	De acuerdo
Mapa de cableado estructurado desactualizado	El Área de Infraestructura y Soporte de TI promoverá el ajuste de los planos del cableado estructurado de acuerdo a las últimas adecuaciones	La Entidad ha estado en constante remodelación y reubicación de personal, tanto que se ha hablado de cambio de sede, así que realizar los planos en este momento no es conveniente
No existe un ambiente de Desarrollo para los sistemas de información y el de Pruebas y Producción no están separados	El Área de Infraestructura y Soporte de TI designara personal necesario para la separación de los ambientes existentes y configuración del ambiente de Desarrollo	No existe personal disponible para la realización de actividades operativas
No existe control de los medios de almacenamiento masivo utilizados	El Área de Infraestructura y Soporte de TI realizará inventario de los medios masivos asignados a las áreas y restringir el acceso a los puertos USB evitando el uso de medios de almacenamiento no incluidos en el inventario	De acuerdo
No existe un mecanismo de destrucción de medios	El Área de Infraestructura y Soporte de TI definirá un procedimiento de destrucción de medios utilizando métodos válidos de sobre escritura como formateo de bajo nivel para proceder a la desintegración o incineración. Adicionalmente determinar por cada medio removible su tiempo de vida, para así poder resguardar la información que contenga	De acuerdo
Uso de software no autorizado	El Área de Infraestructura y Soporte de TI realizará seguimiento periódico a la instalación de software no autorizado como programas de mensajería instantánea	De acuerdo
No existe un mecanismo de Monitoreo de auditoría	El Área de Infraestructura y Soporte de TI analizará ventajas y desventajas de las herramientas existentes en el mercado para determinar la más adecuada para las necesidades de la Entidad	De acuerdo
No se mantiene el uso de contraseñas seguras	El Área de Infraestructura y Soporte de TI incrementará los niveles de complejidad en la definición de contraseñas	De acuerdo
La conexión de portátiles a la red de datos no es controlada	El Área de Infraestructura y Soporte de TI configurará los equipos portátiles de uso interno de tal manera que su conexión a la red inalámbrica sea detectada y restringida. Así como definir el procedimiento para la autorización de conexión a los equipos externos	De acuerdo
Identificación de equipos en la red no estandarizados	El Área de Infraestructura y Soporte de TI realizará un barrido de los equipos conectados a los diferentes segmentos de red, de tal manera que los nombres identifiquen su ubicación	De acuerdo

Tabla 12. (Continuación)

SITUACIÓN ACTUAL	RECOMENDACIÓN	COMENTARIOS
Tiempo de inactividad de sesión muy prolongado	El Área de Infraestructura y Soporte de TI disminuirá al máximo el tiempo de inactividad para inicio de sesión y adelantará campañas de concientización a los funcionarios sobre las medidas de seguridad al ausentarse de sus puestos de trabajo	De acuerdo
Falta de contratos de mantenimiento para el Centro de Datos	El Área de Infraestructura y Soporte de TI adelantará las actividades necesarias para dar continuidad al mantenimiento de aires acondicionados y sistema contra incendios para el Centro de Datos	De acuerdo

Fuente: Autor

Conclusiones:

El plan de trabajo establecido desde hace aproximadamente un año para la implementación del Sistema de Gestión de Seguridad de la Información ha sido adecuado y acorde al tiempo y personal designado para su implementación. Existe un alto porcentaje de controles exigidos por la norma, los cuales están implementados; el área debe fortalecer la parte documental, actualización de guías y procedimientos; normalizar su planta de personal de acuerdo a los cargos disponibles y altas cargas operativas.

Se emite un concepto NO FAVORABLE de acuerdo a las evidencias y resultado de la auditoría.

CONCLUSIONES

Se han implementado muchas medidas de seguridad dando alcance a la norma de acuerdo a la operatividad y criticidad de la información en la medida en que se ha requerido pero no apoyados en un plan de seguridad en profundidad o por capas.

La falta de personal ha retrasado la implementación de controles ya definidos de acuerdo al plan de trabajo sobre la implementación del Sistema de Gestión de Seguridad de la Información.

El control de acceso es uno de los dominios que deben fortalecerse en el área de Infraestructura y Soporte de TI, iniciando con la creación y monitoreo de los sistemas de información generados.

Se aplican procedimientos implícitos en la operatividad del área, basados fundamentalmente en la base de conocimiento del personal pero no se encuentran documentados.

BIBLIOGRAFÍA

ADMINISTRACIÓN ELECTRÓNICA. (2012). Magerit – Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I Método. Madrid, Ministerio de Hacienda y Administración Públicas. Disponible en: http://administracionelectronica.gob.es/pae_Home#.VXMsrdJ_P_g

ADMINISTRACIÓN ELECTRÓNICA. (2012). Magerit – Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II Catálogo de elementos. Madrid, Ministerio de Hacienda y Administración Públicas. Disponible en: http://administracionelectronica.gob.es/pae_Home#.VXMsrdJ_P_g

ADMINISTRACIÓN ELECTRÓNICA. (2012). Magerit – Metodología de análisis y gestión de riesgos de los sistemas de información. Libro III Guía de Técnicas. Madrid, Ministerio de Hacienda y Administración Públicas. Disponible en: http://administracionelectronica.gob.es/pae_Home#.VXMsrdJ_P_g

ALMANZA, Andres. (2013). Revista Sistemas. *Encuesta Seguridad Informática en Colombia, tendencias 2012-2013.* Disponible en: http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-no-127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013

ARROYO, Miguel. (2013). Servicios y Consulting Proxy. *La importancia de la auditoría de seguridad informática*. Disponible en: http://www.proxyconsulting.es/?p=85

AUDIINFORMATICA.COM. Historia de seguridad informática. Disponible en: http://audi-informatica.blogspot.com/

BLOG CERTIFICACION27001. Procesos de certificación ISO 27001. Disponible en: http://certificacion27001.blogspot.com/2010/09/empresas-certificadas-de-colombia.html

COPNIA. (2014). Gestión de medios removibles. Disponible en: https://copnia.gov.co/uploads/filebrowser/DCALIDAD/Sistematizacion/SI-pr-07%20Gesti%C3%B3n%20de%20medios%20removibles.pdf

DECRETO No. 4155 (2011). Por el cual se transforma la Agencia Presidencial para la Acción Social y la Cooperación Internacional, Acción Social, en Departamento Administrativo para la Prosperidad Social, perteneciente al Sector Administrativo de Inclusión Social y Reconciliación, y se fija su objetivo y estructura. Departamento Administrativo de la Función Pública.

Definicionabc.com. (2015). Definición de información. Disponible en: http://www.definicionabc.com/tecnologia/informacion.php

Elespectador.com. (Noviembre 2014). Colombia, líder en inseguridad informática en A. Latina**.** Disponible en: http://www.elespectador.com/tecnologia/colombia-lider-inseguridad-informatica-latina-articulo-482097

HERNÁNDEZ PINTO, Maria Gabriela. (2006). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. Disponible en:https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.dspace.espol.edu.ec%2Fbitstream%2F123456789%2F10730%2F5%2FTESIS%2520Mar%25C3%25ADa%2520Gabriela%2520Hern%25C3%25A1ndez%2520Pinto.doc&ei=Ahh2Ve6LM4fmsASKy4GwDQ&usg=AFQjCNHbWZ7fITBCnJ9Jand0WQJ0eLymXA&sig2=eoaBlPH7aHGPPdUvVWeagw&bvm=bv.95039771,d.cWc

ICONTEC. (2002). NTC-ISO 19011. Directrices para la auditoría de los sistemas de gestión de calidad y/o ambiental. Bogotá, 39 p.

ICONTEC. (2008). NTC 1486. Presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá.Sexta edición, 36p.

ICONTEC. (2007). NTC-ISO-IEC 27002. Código de práctica para la Gestión de la Seguridad de la Información. Bogotá, 132 p.

ICONTEC. (2013). NTC-ISO-IEC 27001. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá.Primera actualización, 26 p.

ISOCALIDAD2000. (2013). Que debería contener un informe de auditoría interna. Disponible en: http://isocalidad2000.com/2013/08/30/que-deberia-aparecer-en-el-informe-de-auditoria-interna-tengo-que-hacer-una-auditoria-interna-y-no-se-por-donde-empezar-xii/

IT GOVERNANCE INSTITUTE. (2007). *Cobit 4.1*. Disponible en: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

CANO, Jeimy, Ph.D. (2008). Seguridad Informática en Colombia. Tendencias 2008. Recuperado de http://www.acis.org.co/fileadmin/Revista_105/investigacion.pdf

KOSUTIC, Dejan. (2012). Ciberseguridad en 9 pasos: El manual sobre seguridad de la información para el gerente. Croacia: EPPS Services Ltd. 6

Mavixel.com. (2014). Los pilares de la seguridad informática. Disponible en: http://www.mavixel.com/video/pilares-seguridad.htm

Metodología para realizar auditoría informática. Disponible en: http://auditordesistemas.blogspot.com/2011/11/metodologia-para-realizar-auditoria.html

MINISTERIO DE SALUD, Gobierno de Chile (2014). Procedimiento para la eliminación segura y reutilización de equipos. Disponible en: http://web.minsal.cl/sites/default/files/files/2014%20Procedimiento%20eliminaci%C3%B3n%20segura.pdf

NORMAS-ISO.com. (2014). ISO 22301 La importancia de estar preparados ante incidentes informáticos: ISO 22301 Sistemas de Gestión de Continuidad del Negocio. Disponible en: http://www.normas-iso.com/2014/iso-22301-continuidad-del-negocio

OPENSOURCE NAC SOLUCION. Principales beneficios de OpenNac. Disponible en: http://www.opennac.org/opennac/en/about/why-opennac.html

ORGANIZACIÓN INTERNACIONAL DE ESTÁNDARES- ISO. Sistema de Gestión de la Seguridad de la Información. Portal ISO 27001 en español. Recuperado de http://www.iso27000.es

REAL ISMS. Guía de referencia de uso. Disponible en: https://sites.google.com/a/realiso.com/realisms-spa/gestao-de-risco/-3-3-ativos-de-informacao

SÁNCHEZ, Esmeralda. (Noviembre 2009). Calidad y seguridad de la información. Y auditoría informática. Disponible en: http://e-archivo.uc3m.es/bitstream/handle/10016/8510/proyectoEsmeralda.pdf?sequence=1

SEGU.INFO.COM (s.f). Seguridad informática – implicancias e implementación. Disponible en: http://www.segu-info.com.ar/tesis/

SUAREZ SIERRA, Lorena. (2013). Sistema de Gestión de la Seguridad de la Información – SGSI.

UF UNIVERSITY OF FLORIDA. (2012). Marco teórico sobre sistemas, auditoría forense, contabilidad, auditoría y estados financieros. Disponible en: http://wwwisis.ufg.edu.sv/wwwisis/documentos/TE/615.109%202-F634a/615.109%202-F634a-CAPITULO%20II.pdf

UNE-ISO/IEC 27002:2009. Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información.

zegurit.blogspot.com. Proyecto de Seguridad Informática. Disponible en: http://zegurit.blogspot.com/

27001ACADEMY. (Agosto 2014). Lista de documentación obligatoria para ISO 22301. Disponible en: http://www.iso27001standard.com/wp-content/uploads/2014/08/Checklist_of_ISO_22301_Mandatory_Documentation_ES.pdf

Anexo A. Checklist Seguridad en Centro de datos

LISTA DE CHEQUEO CONDICIONES DE SEGURIDAD ACTIVOS DE INFORMACIÓN DEL CENTRO DE DATOS

A continuación encontrará preguntas relacionadas con la seguridad de los Activos de Información existentes en el Centro de Datos existente en el segundo piso, oficina de Infraestructura y Soporte de TI

Nombre: _____
Cargo: _____
Fecha: _____

1. Existe un firewall en el esquema perimetral:
   ____NO ____SI

2. Si lo hay, hay disponibilidad de recurso humano para su administración?
   ____NO ____SI

3. Se han presentado incidentes de seguridad que afecte el normal funcionamiento de los servicios en la Entidad?
   ____NO ____SI

   Mencione algunos_____
   _____

4. Con qué frecuencia la Entidad se ha quedado sin servicios que provee el Centro de Datos?
   ____Semanal
   ____Mensual
   ____Semestral
   ____Anual

5. Existe un procedimiento de BackUp para las bases de datos?
   ____NO ____SI

6. Con qué periodicidad se realiza el procedimiento de BackUp?
   ____Diario
   ____Semanal
   ____Mensual
   ____Otro Cual?_____

7. Qué mecanismos de almacenamiento utiliza la entidad?
   ____Servidor
   ____Medio extraíbles (Cintas, Discos, USB, etc)
   ____Otro Cual? _____

8. Qué mecanismos se usan para garantizar la seguridad de las bases de datos?
   _____
   _____

9. Como se realiza mantenimiento a las bases de datos?
   _____
   _____

Anexo B. Cuestionario seguridad en bases de datos

Cuestionario Seguridad en bases de datos

Las preguntas definidas en el siguiente cuestionario hacen relación a las medidas de seguridad contempladas en las bases de datos

Nombre: _____
Cargo: _____
Fecha: _____

1. Qué motores de bases de datos existen en el área y mencione las medidas de seguridad implementadas
2. Como se desarrolla el control de acceso a las bases de datos
3. Que procedimientos o políticas existen para garantizar la seguridad de las bases de datos
4. Qué mecanismos se emplean para el mantenimiento de las bases de datos
5. Que procedimientos o políticas están asociados a éste mantenimiento
6. Qué nivel de privilegios se manejan

Anexo C. Manual de políticas y lineamientos de seguridad de la información

OFICINA DE TECNOLOGIAS DE LA INFORMACION

MANUAL DE POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Advertencia

El presente documento es de uso interno y contiene información acerca de la infraestructura tecnológica, los procedimientos y las políticas de seguridad de la información del Departamento Administrativo para la Prosperidad Social DPS.

Quién tenga acceso a este documento debe tomar todas las medidas necesarias para evitar que la información contenida en este documento no sea revelada a terceros no autorizados, ni sea utilizada para propósitos diferentes al desarrollo de los planes de implementación de los controles de seguridad de la información del DPS.

El incumplimiento de ésta restricción de confidencialidad constituye falta grave que puede conllevar a sanciones administrativas o legales.

INTRODUCCION

El principal activo o valor de una Entidad, es sin duda la información. Es por ello que se debe propender por preservar sus valores y brindarle la protección adecuada. La información se encuentra en diferentes formas (escrita en papel, impresa, almacenada electrónicamente, transmitida por correo, en videos o mediante una conversación), por lo cual sin importar el medio en el cual se encuentra siempre debe estar salvaguardada.

Bajo esta condición, se debe establecer un conjunto de políticas que sirvan como herramientas para la protección de los activos de información. Las políticas de seguridad proveen la base para la implementación de controles de seguridad que reducen los riesgos del sistema, las cuales se deben desarrollar con base en los objetivos y planes estratégicos de la Entidad, siendo consecuentes con sus reglamentos y con los parámetros legales tanto internos y obligatorios que debe cumplir como entidad del estado.

Las políticas deben revisarse periódicamente y mantenerse actualizadas de acuerdo a los requerimientos organizacionales y a los requerimientos legales.

Las políticas deben ser divulgadas y socializadas debidamente mediante los canales y medios que tiene la Entidad como circulares, acuerdos, resoluciones, contratos y herramientas de divulgación como Intranet, correos, carteleras. Debe quedar constancia del conocimiento y entendimiento de las políticas por parte de las personas a las que apliquen estas directrices.

La Seguridad de la Información es una prioridad para el DPS y por lo tanto es responsabilidad de todos los funcionarios y Colaboradores de la Entidad velar por el continuo cumplimiento de las políticas definidas.

ALCANCE

Las Políticas Generales establecidas en este Documento rigen para todos los funcionarios y Colaboradores del Departamento Administrativo para la Prosperidad Social DPS y deberán ser acatadas por todas aquellas personas que en el ejercicio de sus labores interactúen con los servicios y recursos de la Entidad tanto en forma directa como indirecta (Proveedores, Consultores y Asesores, usuarios externos u otros terceros).

ESTRUCTURA DEL DOCUMENTO

Este Documento de políticas, está estructurado de acuerdo a los Objetivos de Control y Controles establecidos en la norma **NTC- ISO-IEC 27001: 2013**. Es así como el presente documento se encuentra directamente relacionado con el anexo A de la norma, iniciando desde el dominio de

Aspectos Organizativos de Seguridad dela Información y finalizando en el dominio de Cumplimiento de los Requisitos Legales; por ello sus títulos están alineados con dicho anexo en los objetivos de control y controles para los cuales la entidad ha fijado políticas de seguridad de la información.

GLOSARIO DE TÉRMINOS

Activo de Información: Se entiende por activo de Información todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la Entidad. Ej. Información de bases de datos, programas de computación, plataforma tecnológica (procesamiento de datos o comunicaciones), documentos impresos y Recursos Humano.

Análisis de riesgos: Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

Archivo .OST: Archivo Binario de Carpetas personales con conexión fuera de línea.

Archivo .PST: Archivo binario de carpetas personales que almacena mensajes, eventos de calendario, entre otros.

Carpetas Personales de Outlook: Estructura de correo en Outlook que corresponde a un archivo de tipo .PST o .OST.

Colaborador: Se entiende por Colaborador, a toda persona que tenga vínculo laboral como funcionario o contrato por prestación de servicio con la Entidad.

Confidencialidad: Asegurar que la información está disponible solamente para los usuarios autorizados a tener acceso a dichos datos.

Control: Una forma para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Cuenta institucional: Cuenta de la entidad que no hace referencia al nombre de un usuario si no de un área, grupo o de acuerdo a una necesidad.

Disponibilidad: Asegurar que los usuarios tengan, en todo momento, la información a la cual tienen derecho.

Dispositivo Móvil: Se entiende por todo dispositivo incluido dentro del concepto de movilidad debido a que es ser portable y utilizable durante su transporte. Dentro de estos dispositivos se incluyen: teléfonos celulares, Smartphones, computadores portátiles, tabletas, etc.

Evento de Seguridad de la Información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Incidente de Seguridad de la Información: Se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Información: es un conjunto organizado de datos.

Integridad: Asegurar que la información es adecuada y apropiada para su procesamiento.

Seguridad de la Información: Salvaguardarla confidencialidad, integridad y disponibilidad de la información.

SPAM: Correo no deseado de tipo basura o potencialmente peligroso.

Terceros: Se entiende por tercero a toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad, o entre los cuales medie convenio, contrato o relación alguna.

Usuario: Colaborador del DPS, tanto de planta como de contrato, que hace uso de un equipo computacional o de un sistema de información.

POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Aspectos Organizativos de la Seguridad de la Información

I. Política de Organización Interna

Objetivo: Garantizar el soporte operativo para las actividades de seguridad de la información en el DPS

Roles y responsabilidades

1. Todos los Colaboradores del DPS, proveedores o contratistas, así como los terceros autorizados para acceder a la infraestructura de procesamiento de información, serán

responsables del cumplimiento de las políticas, procedimientos y estándares definidos por la Entidad.

2. La información almacenada en los equipos de cómputo de la Entidad es propiedad del DPS y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

3. Todos los Colaboradores del DPS deberán mantener especial cuidado de no divulgar información CONFIDENCIAL o RESERVADA en lugares públicos o privados, mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la organización. Esta restricción se extiende inclusive con posterioridad a terminación del vínculo laboral o terminación de los contratos y debe estar incluida en los Acuerdos de Confidencialidad.

4. Todos los activos de información del DPS deben tener claramente identificado su propietario y su custodio.

5. Únicamente los dueños de procesos estratégicos, misionales o de apoyo, de acuerdo al mapa de procesos del DPS, pueden ejercer el rol de propietarios de activos de información. En este caso el propietario es el encargado de tomar las decisiones claves sobre dicho activo y se apoya en el custodio para su protección en términos de seguridad.

6. Los Colaboradores que ejercen el rol de custodios de algún activo de información del DPS, actúan como responsables de proteger el activo en términos de confidencialidad, integridad y disponibilidad, por lo tanto debe informarse acerca de las medidas necesarias para proteger el activo.

Seguridad de la información en gestión de proyectos

1. La metodología de gestión de proyectos empleada por el DPS debe considerar la seguridad de la información como un componente transversal y por lo tanto debe incluirla desde el inicio del proyecto y durante su ejecución. Esto aplica a cualquier tipo de proyecto.

2. Como parte de los objetivos definidos para los proyectos desarrollados, se deben incluir objetivos de seguridad de la información acordes con la información que va a ser manejada a lo largo del proyecto.

3. En las etapas iniciales de un proyecto como parte de los riesgos asociados al proyecto, se debe incluir una identificación y evaluación de riesgos de seguridad de la información, para los cuales se deben definir controles de seguridad que aporten a su mitigación.

4. La responsabilidad sobre la implementación y la efectividad de los controles de seguridad aplica sobre el gerente de proyectos o supervisor del contrato de implementación.

II. Política de Dispositivos Móviles

Objetivo: Proteger la información del DPS que se encuentra almacenada en dispositivos móviles y gestionar sus riesgos asociados

1. El uso de los equipos portátiles de propiedad del DPS fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante una orden de salida, la cual debe tener el visto bueno del delegado de los procesos con firma autorizada para este fin.

2. Los equipos que estén autorizados para salir y que contengan información sensible, se deben proteger mediante el uso de uno o varios de los siguientes controles tecnológicos:

   - Antivirus.
   - Encriptación de datos.
   - Restricción en la ejecución de aplicaciones.
   - Restricción de conexión de dispositivos USB.
   - Protección física mediante la guaya de seguridad.
   - Desactivar accesos inalámbricos cuando se encuentren conectadas a la red LAN

3. Cualquier dispositivo móvil que albergue información del DPS debe poseer un sistema de autenticación, basado al menos en un patrón de movimiento, un código de desbloqueo o una contraseña.

4. Cualquier dispositivo móvil que albergue información del DPS debe tener instalado un software de antivirus.

5. Los dispositivos móviles que son propiedad del DPS pueden estar sometidos a un control sobre el tipo y la versión de aplicaciones instaladas, al igual que pueden estar sometidos a restricciones de conexión hacia ciertos servicios de información que sean considerados maliciosos.

6. Los dispositivos móviles que son propiedad de los funcionarios, pueden tener almacenada información del DPS, como el correo electrónico, siempre y cuando dichos equipos se encuentren registrados e identificados y se implementen las medidas de aseguramiento definidas por el GT de Infraestructura y Soporte de TI para garantizar la preservación de la confidencialidad e integridad de la información del DPS.

7. En caso de pérdida o robo de un dispositivo móvil que contenga información del DPS, el funcionario a cargo del dispositivo móvil, debe avisar inmediatamente al GT de Infraestructura y Soporte de TI, quien está en libertad para iniciar un proceso de borrado remoto de información. (Ver Formato de Aceptación de Condiciones para la Instalación de Correo Electrónico en Dispositivos Móviles).

III. Política de Teletrabajo

Objetivo: Proteger la información del DPS accedida desde lugares donde se realiza teletrabajo.

1. Las solicitudes de acceso remoto a equipos de cómputo o servicios de procesamiento de información de la red interna del DPS, deben contar con el aval del propietario del proceso al cual pertenece el funcionario solicitante del acceso.

2. Las solicitudes de acceso remoto serán configuradas principalmente para acceder por escritorio remoto únicamente al equipo de escritorio que ha sido designado al funcionario en las instalaciones del DPS, evitando de esta forma el procesamiento y almacenamiento de información del DPS en equipos de terceros. En la situación, en la que el funcionario no cuente con un equipo de escritorio en las instalaciones del DPS, se habilitarán accesos a servicios de procesamiento de información individuales, basados siempre en una justificación de la necesidad de acceso (Ver Formato de Solicitud de Conexión Remota).

3. Las solicitudes de acceso remoto a equipos de cómputo diferentes del equipo de escritorio que ha sido designado al funcionario en las instalaciones del DPS, deben contar con la aprobación del propietario del activo de tipo información primario almacenado en el equipo de cómputo al cual se desea tener acceso, por ejemplo para el acceso remoto a un servidor de inteligencia de negocios, se debe contar con la aprobación del funcionario que hace las veces de propietario de la información almacenada en dicho servidor.

4. Las solicitudes de acceso remoto a equipos de cómputo o servicios de procesamiento de información deben indicar siempre un tiempo de duración del acceso remoto, siendo tres (3) meses el tiempo máximo para una solicitud. En caso de que este tiempo no se especifique, se asumirá un tiempo de duración del acceso remoto de una (1) semana (Ver Formato de Solicitud de Conexión Remota).

5. Posterior al tiempo de duración del acceso remoto, el acceso remoto será revocado hasta que se haga una nueva solicitud de acceso. La revocación exige la creación de unas nuevas credenciales de acceso para el usuario solicitante.

6. Los accesos remotos se deben configurar considerando siempre: conexiones cifradas, tiempos de sesión y autenticación a nivel de usuario. Para este propósito, el mecanismo autorizado son conexiones de tipo VPN (Virtual Private Network).

7. El funcionario solicitante del acceso remoto es responsable del uso indebido o no autorizado que se haga con el acceso remoto que le ha sido designado, incluyendo el que realicen otros usuarios con acceso al equipo de cómputo desde el cual se hace el acceso remoto.

8. El DPS tiene potestad para verificar las características operativas y de seguridad de equipos de cómputo de terceros desde los cuales se hace el acceso remoto. En caso de encontrarse condiciones no óptimas, el acceso remoto puede ser negado o revocado, indicándose la justificación que condujo a dicha decisión.

9. Los accesos remotos están sujetos a monitoreo, el cual incluye hora y duración de la conexión, datos transmitidos o recibidos hacia o desde la infraestructura del DPS, direcciones IP de origen de la conexión, etc.

10. El usuario solicitante deberá recibir las indicaciones adecuadas para hacer la correcta instalación del software requerido para el acceso de tipo VPN. (Ver Instructivo de Configuración de Acceso Remoto por VPN).

Seguridad de los Recursos Humanos

I. Política de Seguridad de los recursos humanos

Objetivo: Proteger la información del DPS por medio de la validación, formación y concientización del recurso humano que hará uso de la misma.

Selección de personal

1. Dentro de los procesos de contratación de personal o de prestación de servicios, deberá realizarse la verificación de antecedentes cuando así lo amerite y en los casos que se considere necesario se debe contemplar la realización del estudio de seguridad. Esto aplica especialmente cuando el Colaborador vaya a tener acceso a información del DPS que haya sido clasificada como CONFIDENCIAL o RESERVADA.

2. La Subdirección de Talento humano es la responsable de realizar la verificación de antecedentes, para lo cual puede llevar a cabo cualquiera de las siguientes actividades:

verificación de referencias personales y laborales, validación de la hoja de vida del aplicante, confirmación de calificaciones académicas y profesionales, revisión de documentación de identidad alterna (pasaporte, tarjeta de conducción, etc.), revisión de antecedentes criminales, etc.

Términos y condiciones Laborales

1. Todos los Colaboradores del DPS debe cumplir con los requerimientos de seguridad de la información y estos debe hacer parte integral de los contratos o documentos de vinculación a que haya lugar, para ello se firmará el documento Acuerdo Individual de Confidencialidad (Ver Formato Acuerdo Individual de Confidencialidad) donde se evidencie el conocimiento y aceptación del documento "Documento de Políticas y Lineamientos de seguridad de la información".

2. Todos los Colaboradores, durante el proceso de vinculación al DPS, deberán recibir una inducción sobre las Políticas de Seguridad de la Información.

Entrenamiento, concientización y capacitación

1. Los Colaboradores del DPS deben ser entrenados y capacitados para las funciones/actividades y cargos a desempeñar con el fin de proteger adecuadamente los recursos y la información de la institución; y garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá extenderse al personal de contratistas o terceros, cuando sus responsabilidades así lo exijan.

Procesos disciplinarios

1. A todos los incidentes de seguridad de la información ocurridos en el DPS se le debe dar el tratamiento respectivo con el fin de determinar sus causas y responsables. De los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta la gravedad y responsabilidades identificadas, se tomarán acciones y se realizará el respectivo trámite ante las instancias correspondientes.

Gestión de Activos

I. Política de uso de correo electrónico.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información del DPS en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Usos aceptables del servicio

1. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el DPS, no debe utilizarse para ningún otro fin, así mismo se deberá utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información del DPS.

2. Los usuarios autorizados para usar el servicio de correo electrónico son responsables de todas las actividades realizadas con sus usuarios de acceso a los buzones de correo, así como de mantener un comportamiento ético y acorde a la ley (especialmente las actividades delictivas mencionadas en Ley 1273 de 2009), y de evitar prácticas o usos que puedan comprometer la seguridad de la información del DPS.

3. El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con el DPS. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad del DPS y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de investigaciones o incidentes de seguridad de la información.

4. Cuando un Proceso, Programa o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones del DPS.

5. Todos los mensajes enviados deberán respetar el estándar de formato e imagen corporativa definido por el DPS y deberán conservar en todos los casos el mensaje legal corporativo.

6. El único servicio de correo electrónico controlado en la entidad es el asignado directamente por el Grupo de Trabajo de Infraestructura y Soporte de TI, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene respaldo de diferentes procesos de copia de

respaldo (backup) aplicados de manera periódica y segura. Los demás servicios de correo electrónico serán utilizados a cuenta y riesgo de los usuarios, siendo necesaria la aprobación y firma por parte del Director, Jefe de Oficina, Subdirector o Coordinador de Grupo de Trabajo; de un documento de análisis de riesgos para la autorización de sistemas de correo electrónico diferentes al institucional.

7. El servicio de correo electrónico debe prestarse siempre por medio de un canal cifrado. Este control está a cargo del Grupo de Trabajo de Soporte e Infraestructura.

8. Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado, Confidencial) según lo definido en el documento Guía de Clasificación y Etiquetado de la Información. Igualmente los adjuntos deben estar etiquetados de acuerdo a lo establecido en dicha guía.

9. El tamaño del buzón de correo electrónico se asignará de manera estandarizada, la capacidad específica será definida y administrada por el Grupo de Trabajo de Infraestructura y Soporte de TI.

10. Todo usuario es responsable de informar si tiene acceso a contenidos o servicios que no le estén autorizados y no correspondan a sus funciones/actividades designadas dentro del DPS, para que de esta forma el Grupo de Trabajo de Infraestructura y Soporte de TI realice el ajuste de permisos requerido.

11. El usuario deberá informar cuando reciba correos de tipo SPAM, correo no deseado o no solicitado, correos de dudosa procedencia o con virus, al Grupo de Infraestructura y Soporte de TI, para que este tome la medidas pertinentes y acciones que impidan el ingreso de ese tipo de correo. De la misma forma el usuario deberá informar al Grupo de Trabajo de Infraestructura y Soporte de TI, cuando no reciba correo y este seguro que este no es de tipo SPAM, de esta forma el Grupo de Trabajo de Infraestructura y Soporte de TI evaluará el origen y tomará las medidas pertinentes.

12. Cuando un Colaborador al que le haya sido autorizado el uso de una cuenta de acceso a la red y al servicio de correo corporativo se retire del DPS, deberá abstenerse de continuar empleándolas y deberá verificar que su cuenta y acceso a los servicios sean cancelados.

13. Los mensajes y la información contenida en los buzones de correo son de propiedad del DPS. Los buzones no deberán contener mensajes con antigüedad superior a un (1) año. El usuario podrá crear un histórico de su correo siempre y cuando sea local (almacenado en el disco duro del usuario) y bajo su propia responsabilidad.

14. Para el uso del servicio de correo electrónico, el usuario se debe guiar por lo establecido en

el Protocolo de Comunicaciones del DPS.

15. Cada usuario se debe asegurar que en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a las personas apropiadas. Si tiene listas de distribución se deben depurar en el mismo sentido. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

16. La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Usos no aceptables del servicio

1. Este servicio no debe ser usado para:
    - Envío de correos masivos que no hayan sido autorizados por un propietario de un proceso misional, estratégico o de apoyo, de acuerdo al mapa de procesos del DPS.
    - Envío, reenvío o intercambio de mensajes no deseados o considerados SPAM, cadena de mensajes o publicidad.
    - Envío de correos con archivos adjuntos de tamaño superior a la cuota permitida (Quince (15) Mb).
    - Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.
    - Envío o intercambio de mensajes que promuevan la discriminación sobre la base de raza, género, nacionalidad de origen, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.
    - Envío de mensajes que contengan amenazas o mensajes violentos.
    - Creación, almacenamiento o intercambio de mensajes que violen las leyes de material protegido por la Ley de derechos de autor.
    - Distribución de información del DPS, no PÚBLICA, a otras entidades o ciudadanos sin la debida autorización.
    - Crear, enviar, alterar, borrar mensajes de otro usuario sin su autorización.
    - Apertura, uso o revisión indebida de la cuenta de correo electrónico de otro usuario como si fuera propia sin la debida autorización.
    - Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

- Adulterar o intentar adulterar mensajes de correo.
- Enviar mensajes de correo utilizando la cuenta de correo de otra persona exceptuando la administración de calendarios compartidos cuando el Jefe inmediato lo autorice.
- Enviar correos masivos, con excepción de funcionarios con nivel de Director o superior, quienes sean previamente autorizados por estos para ello, o de funcionarios que en calidad de sus funciones amerite la excepción.
- Intentar acceder a una cuenta de correo de otro usuario o a carpetas y archivos de otra persona sin su autorización. A menos que exista una investigación, un incidente de seguridad de la información o un problema reportado por el usuario.
- Enviar información Confidencial o Reservada del DPS a personas u organizaciones externas, salvo en los casos expresamente previstos en la Constitución Política y en la Ley, y por parte de los funcionarios autorizados internamente para ello.

Condiciones de uso del servicio

1. La configuración del archivo de carpetas de datos personales en el equipo asignado deberá ser regularmente del tipo .PST para todos los usuarios y por excepción del tipo .OST.

2. El servicio de correo electrónico notificará automáticamente (vía correo electrónico) a los usuarios cuando su buzón haya o este por alcanzar su límite. El tamaño de los buzones por defecto es de 300 MB.

3. El usuario será el responsable de la no entrega y/o recepción de mensajes en su buzón cuando se supere la cuota de almacenamiento.

4. Existirán excepciones de capacidad para ciertos buzones que tenga una cuota mayor como el caso de los directores o algunos buzones especiales pero en ningún caso se superará la cuota de 1 GB.

5. Las cuentas institucionales (Ejemplo: Comunica, Servicio al Ciudadano, Soporte, etc.) deben tener una persona responsable que haga depuración del buzón.

6. El password o clave de acceso al servicio es la mejor defensa contra el uso no autorizado de la cuenta de acceso al servicio y/o a la red de datos del DPS por lo tanto se requiere que se mantenga en la mayor reserva posible, no debe suministrarse a otras personas o exhibirse en público.

7. El DPS puede supervisar cualquier cuenta de correo institucional para certificar que se está

usando para los propósitos legítimos. El incumplimiento de esta política puede conducir a acciones disciplinarias tales como terminación de la relación laboral o contractual.

8. Todo usuario es responsable por la destrucción de todo mensaje cuyo origen es desconocido, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Colaborador desconfíe del remitente de un correo electrónico debe remitir la consulta al correo de seguridad de la información del Grupo de Trabajo de Soporte e Infraestructura (seguridaddelainformacion@dps.gov.co).

9. Si una cuenta de correo es capturada por hackers o se reciben excesiva cantidad de correo no deseado (SPAM), el Grupo de Trabajo de Infraestructura y Soporte de TI tiene libertad para generar una nueva cuenta y borrar la anterior.

10. En caso de que el tamaño de los archivos adjuntos sea muy grande, se recomienda que se compacten o se dividan para evitar que se tengan inconvenientes de recepción o envió. Así también se evitaría el consumo innecesario de recursos.

11. Los Usuarios deben ser conscientes de los riesgos legales que implica la utilización de los medios electrónicos, especialmente en cuanto a la responsabilidad disciplinaria, penal y/o civil en la que pueden incurrir por los inconvenientes, perjuicios y/o reclamaciones de cualquier tipo que llegaren a presentarse como resultado de cualquiera de las siguientes conductas, entre otras:
    - Enviar o reenviar información sensible, sin estar legalmente autorizado para ello.
    - Reenviar o copiar sin permiso mensajes "Confidenciales" o protegidos por las normas sobre derechos de autor, o contra expresa prohibición del originador.

12. El grupo de soporte de TI se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no puede ser eliminado, el mensaje será borrado.

13. El usuario debe evitar suscribirse en boletines en líneas con el correo institucional, para evitar la llegada de cadenas de correo, publicidad, etc.

14. Las listas de distribución son administradas por el responsable del grupo de soporte de TI y para su creación se requiere autorización del jefe inmediato.

15. El usuario no debe responder mensajes donde le solicitan información personal o financiera para participar en sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda

humanitaria. Estas situaciones se deben informar al Grupo de Infraestructura y Soporte de TI con el fin de bloquear dicho remitente y evitar que esos mensajes lleguen a más funcionarios. Igualmente se deben marcar estos mensajes como no deseados desde el cliente de correo.

16. Toda cuenta de correo mantenida en el sistema de correo electrónico es de propiedad del DPS. Las cuentas de correo que no sean utilizadas por más de cuarenta y cinco (45) días podrán ser desactivadas por el Grupo de Infraestructura y Soporte de TI.

17. Los correos electrónicos dirigidos a otros dominios deben contener una sentencia de confidencialidad con un contenido como el siguiente (ejemplo):

    ****
    ****

    CONFIDENCIALIDAD: Este correo electrónico es correspondencia confidencial del Departamento Administrativo para la Prosperidad Social. Si Usted no es el destinatario, le solicitamos informe inmediatamente al correo electrónico del remitente o a seguridaddelainformacion@dps.gov.co,así mismo por favor bórrelo y por ningún motivo haga público su contenido, de hacerlo podrá tener repercusiones legales. Si Usted es el destinatario, le solicitamos tener absoluta reserva sobre el contenido, los datos e información de contacto del remitente o a quienes le enviamos copia y en general la información de este documento o archivos adjuntos, a no ser que exista una autorización explícita a su nombre.

    ****
    ******

    CONFIDENTIALITY: This email is confidential correspondence of Departamento Administrativo para la Prosperidad Social. If you are not the receiver, you are requested to immediately inform the sender or email seguridaddelainformacion@dps.gov.co, likewise please delete it and do not publicize its content for any reason, due to it may have legal repercussions. If you are the receiver, we ask to have absolute secrecy about the content, data and contact information of the sender and in general about the information in this document or attachments, unless there is an explicit consent under your name.

    ****
    *****

    Para todos los usuarios de correo electrónico, el tamaño máximo para recibir o enviar correo será de 15 MB (incluyendo la suma de todos los adjuntos).

Responsabilidades

1. La Subdirección de Talento humano es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Correo electrónico corporativo al Grupo de Trabajo de Infraestructura y Soporte de TI. Cuando se solicite una cuenta institucional se debe justificar e informar de la persona responsable de dicho buzón. Si se detecta que se solicita una cuenta institucional y que no se hace uso de ella, el Grupo de Trabajo de Infraestructura y Soporte de TI podrá eliminar dicha cuenta.

2. Todos los Colaboradores, en el desarrollo de sus tareas habituales u ocasionales que utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que provea el DPS, son responsables del cumplimiento y seguimiento de esta política.

3. El Grupo de Trabajo de Infraestructura y Soporte de TI es el responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario y/o al servicio de Correo electrónico corporativo para los Colaboradores que desempeñen labores o actividades en el DPS.

4. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de monitorear las comunicaciones y/o información que se comuniquen mediante el servicio de correo electrónico corporativo.

5. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de filtrar los contenidos que se trasmitan en la red del DPS y en uso del servicio de Correo electrónico corporativo.

II. Política de uso de Internet.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información del DPS en el uso del servicio de Internet por parte de los usuarios autorizados.

Usos aceptables del servicio

1. Este servicio debe utilizarse exclusivamente para las tareas propias de la función/actividad desarrollada en el DPS y no debe utilizarse para ningún otro fin.

2. Los usuarios autorizados para usar el servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del DPS.

3. El servicio debe ser empleado para servir a una finalidad operativa y administrativa en relación con el DPS. Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control.

Usos no aceptables del servicio

Este servicio no debe ser usado para:

1. Envío y/o descarga de información masiva de gran tamaño que pueda congestionar la red.

2. Envío y/o descarga y/o visualización de información con contenidos que atenten contra la integridad moral de las personas o instituciones.

3. Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

Condiciones de uso del servicio

1. El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con el DPS como colaborador, diligenciando la solicitud de acceso a servicios tecnológicos.

2. El servicio debe utilizarse única y exclusivamente para las tareas propias de la función o actividad desarrollada en el DPS y no debe utilizarse para ningún otro fin.

3. El único servicio de navegación autorizado para el uso de Internet en las Redes del DPS es el provisto directamente por el Grupo de Trabajo de Infraestructura y Soporte de TI, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

4. No se permite la conexión de módems externos o internos, que no estén autorizados por el Grupo de Infraestructura y Soporte de TI.

5. Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña el usuario en el DPS y para los cuales este formal y expresamente autorizado.

6. Todo usuario es responsable de informar de contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones/actividades dentro del DPS.

7. Cuando un colaborador al que le haya sido autorizado el uso de una cuenta de acceso a la red y al servicio de Internet se retire del DPS, deberá abstenerse de continuar empleándolas y deberá verificar que su cuenta y acceso a los servicios sean cancelados.
8. Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier

otra información que se envíe desde la red del DPS o descargue desde Internet.

9. No se permitirá el acceso a páginas relacionadas con pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, pornografía, spyware, adware, redes peer to peer (p2p),o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos del DPS.

10. No se permitirá la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.

11. No se permitirá el intercambio no autorizado de información de propiedad del DPS, de sus usuarios y/o de sus Colaboradores, con terceros.

12. El DPS realizará monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los Colaboradores. Así mismo, el DPS podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación.

13. Cada uno de los Colaboradores será responsable de dar un uso adecuado de este recurso y en ningún momento podrá ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.

14. Los Colaboradores no podrán asumir en nombre del DPS, posiciones personales en encuestas de opinión, foros u otros medios similares.

15. Este recurso podrá ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información del DPS.

Responsabilidades

1. La Subdirección de Talento Humano es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Internet al Grupo de Trabajo de Infraestructura y Soporte de TI.

2. Todos los Colaboradores, en el desarrollo de sus tareas habituales u ocasionales que utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que

provea el DPS, son responsables del cumplimiento y seguimiento de esta política.

3. El Grupo de Trabajo de Infraestructura y Soporte de TI es el responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario y/o al servicio de Internet para los Colaboradores que desempeñen labores/actividades en el DPS.

4. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de monitorear las comunicaciones y/o información que presenten un comportamiento inusual o sospechoso.

5. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de filtrar los contenidos que se reciban desde Internet y/o se envíen desde la red del DPS.

III. Política de uso de Redes Sociales.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información del DPS en el uso del servicio de Redes sociales por parte de los usuarios autorizados.

1. Los usuarios autorizados para usar los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del DPS.

2. El servicio debe ser utilizado para actividades relacionadas con el DPS. Todas las comunicaciones establecidas mediante este servicio pueden ser monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

3. Se permite el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.

4. La Entidad facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento a muchas actividades que se realizan por estos medios, Sin embargo es necesario utilizar este medio de forma correcta y moderada.

5. No se deben descargar programas ejecutables o ficheros que sean susceptibles de contener “software malicioso”.

6. No se permiten descargas, difusión o distribución de material obsceno, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.

7. No se debe intentar violar los sistemas de seguridad del servicio de Internet de la Entidad, o aprovechar el acceso a Redes Sociales para fines ilegales, esto incluye la descarga de software sin el debido permiso de uso dentro de la Entidad.

8. Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

9. Tampoco está autorizado el uso, instalación o manipulación de key-loggers o exploits.

10. No se debe acceder ilegalmente, sin autorización o intentar superar medidas de seguridad de ordenadores o redes que pertenezcan a un tercero (conocido como “hacking”), así como cualquier actividad previa al ataque de un sistema para recoger información sobre este, como por ejemplo, escaneo de puertos.

11. Los Colaboradores del DPS, no deben crear cuentas, abrir grupos, o publicar cualquier tipo de información escrita o audiovisual a nombre del DPS. Cualquier iniciativa que surja en este sentido deberá ser consultada con la Oficina Asesora de Comunicaciones.

12. Todos los Colaboradores que interactúan, en el desarrollo de sus tareas habituales u ocasionales y que utilicen cualquier servicio de tecnología de la información y comunicaciones (TIC) que provea el DPS son responsables del cumplimiento y seguimiento de estas política.

13. El Grupo de Trabajo de Infraestructura y Soporte de TI es el responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario y/o al servicio de Internet para los Colaboradores que desempeñen labores en el DPS.

14. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de monitorear las comunicaciones y/o información que presenten un comportamiento inusual o sospechoso.

15. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de filtrar los contenidos que se reciban desde las redes sociales y/o se envíen desde la red del DPS.

16. Según la disponibilidad de los recursos de transmisión y acceso a internet con los que cuente el DPS, se autorizara el uso y limitaciones en el acceso a las plataformas de redes sociales.

17. El Grupo de Infraestructura y Soporte de TI, será el encardo de determinar las directrices y lineamientos para el uso de los diferentes sistemas o plataformas de redes sociales en la entidad.

Usos no aceptables del servicio

1. Envío y/o descarga de información masiva de gran tamaño que pueda congestionar la red.

2. Envío y/o descarga y/o visualización de información con contenidos que atenten contra la integridad moral de las personas o instituciones.

3. Cualquier otro propósito diferente a las actividades relacionadas con el DPS.

IV. Política de uso de la Intranet

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información del DPS en el uso del servicio de Intranet por parte de los usuarios autorizados.

1. Los usuarios autorizados para usar el servicio de Intranet son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del DPS.

2. El servicio debe ser empleado para servir a una finalidad operativa y administrativa en relación con el DPS. Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control.

Usos aceptables del servicio

1. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en el DPS y no debe utilizarse para ningún otro fin.

Usos no aceptables del servicio

Este servicio no debe ser usado para:

- Envío y/o manejo de información con contenidos que atenten contra la integridad moral de las personas o instituciones.

- Cualquier otro propósito diferente al considerado en el apartado de Uso aceptable del servicio.

Condiciones de uso del servicio

1. El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con el DPS como colaborador.

2. El servicio debe utilizarse única y exclusivamente para las tareas propias de la función desarrollada en El DPS y no debe utilizarse para ningún otro fin.

3. El password o clave de acceso al servicio es la mejor defensa contra el uso no autorizado la cuenta de acceso al servicio y/o a la red de datos del DPS por lo tanto se requiere que se mantenga en la mayor reserva posible, no debe suministrarse a otras personas o exhibirse en público.

4. El único navegador autorizado para el uso del servicio de Intranet en el DPS es el asignado directamente por el Grupo de Trabajo de Infraestructura y Soporte de TI, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

5. Los servicios a los que un determinado usuario pueda acceder desde la Intranet dependerán del rol que desempeña el usuario en el DPS y para los cuales este formal y expresamente autorizado.

6. Todo usuario es responsable de informar de contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones/actividades dentro del DPS.

7. Cuando un colaborador al que le haya sido autorizado el uso de una cuenta de acceso a la red y al servicio de Intranet, se retire del DPS, deberá abstenerse de continuar empleándolas y deberá verificar que su cuenta y acceso a los servicios sean cancelados.

Responsabilidades

1. La Subdirección de Talento Humano es la responsable de solicitar la creación, modificación o cancelación de las cuentas de acceso a la red y al servicio de Intranet al Grupo de Trabajo de Infraestructura y Soporte de TI.

2. El Grupo de Trabajo de Infraestructura y Soporte de TI es el responsable de administrar la plataforma tecnológica que soporta el acceso a la red/cuentas de usuario y/o al servicio de Intranet para los Colaboradores que desempeñen labores/actividades en el DPS.

3. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de monitorear las comunicaciones y/o información que presenten un comportamiento inusual o sospechoso.

4. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de filtrar los contenidos que se trasmitan en la red del DPS y en uso del servicio de Intranet.

V. Política de uso de Recursos Tecnológicos

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información del DPS a través de la definición de las condiciones de uso aceptable de los recursos tecnológicos.

El DPS asignará diferentes recursos tecnológicos como herramientas de trabajo para uso exclusivo de sus Colaboradores autorizados. El uso adecuado de estos recursos se reglamenta bajo las siguientes directrices:

1. La instalación de cualquier tipo de software en los equipos de cómputo del DPS debe ser realizada por el Grupo de Trabajo de Infraestructura y Soporte de TI y por tanto son los únicos autorizados para realizar esta labor.

2. Los usuarios no deberán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios podrán ser realizados únicamente por el Grupo de Trabajo de Infraestructura y Soporte de TI.

3. El Grupo de Trabajo de Infraestructura y Soporte de TI definirá la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

4. Sólo personal autorizado podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del DPS; las conexiones establecidas para este fin, utilizarán los esquemas de seguridad definidos.

5. Los Colaboradores de la Entidad son responsables de hacer buen uso de los recursos tecnológicos del DPS y en ningún momento podrán ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros Colaboradores, terceros, la legislación vigente y las políticas y lineamientos de seguridad de la información del DPS.

5. La información de carácter personal almacenada en dispositivos de cómputo, medios de almacenamiento o cuentas de correo institucionales debe de ser almacenada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como “PERSONAL”.

Devolución de los Activos

1. Todo activo de propiedad del DPS, asignado a un Colaborador de la Entidad o a una tercera parte, deberá ser entregado a la finalización del contrato o por cambio de cargo. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.

VI. Política de Clasificación de la Información

Objetivo: Asegurar que la información del DPS es tratada y protegida adecuadamente de acuerdo al nivel de clasificación otorgado.

Esquema de Clasificación de la Información

1. Toda información perteneciente al DPS deberá ser identificada y clasificada de acuerdo a los siguientes niveles**:**

- Público
- Uso Interno
- Confidencial
- Reservado

2. El Grupo de Trabajo de Infraestructura y Soporte de TI en conjunto con el Proceso de Gestión Documental son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento o de manejo que deben darse a la información en función del nivel de clasificación al que pertenecen. (Ver Guía de Clasificación y Etiquetado de la Información).

3. Para el manejo y almacenamiento de la información acorde a la clasificación establecida anteriormente, es necesario tener en cuenta lo siguiente:

- Restringir el acceso solo al personal debidamente autorizado
- Mantener un registro formal de los receptores autorizados de datos o información
- Conservar los medios de almacenamiento en un ambiente seguro

Etiquetado y manejo de Información

1. Cada colaborador de la Entidad deberá mantener organizado el archivo de gestión, acatando los lineamientos establecidos por el Proceso de Gestión Documental.

2. Los Directores, Jefes de Oficina, Subdirectores o Coordinadores de Grupo deberán establecer mecanismos para el control de la Reprografía de los documentos, con el fin de mantener la integridad y confidencialidad de la información. (Documento físico).

3. Todos los Colaboradores del DPS son responsables de la Organización, conservación, uso y manejo de los Documentos.

4. Las diferentes dependencias del DPS deberán enviar al Archivo Central la documentación en forma ordenada y organizada, de acuerdo a los tiempos de vigencia estimados en la Tabla de Retención documental, acompañada del documento formato F-AAD-005 Transferencia documental, y en medio magnético.

5. El Archivo Central recibirá las transferencias documentales de acuerdo al calendario anual de transferencia Documentales.

6. Los archivos de Gestión de las dependencias u oficinas de la institución deberán custodiar sus documentos de acuerdo a lo especificado en la correspondiente tabla de retención Documental.

7. La tecnología utilizada para salvaguardar, facilitar y conservar la información de los documentos en soportes informáticos debe garantizar la seguridad de no permitir alteraciones o consultas de personas no autorizadas.

Administración de los Archivos

1. Los Colaboradores del DPS al desvincularse de las funciones/actividades titulares entregarán los documentos y archivos a su cargo debidamente inventariados.

2. Es deber de todo colaborador del DPS, custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
3. A todo colaborador del DPS le está prohibido:
    - Omitir, retardar o no suministrar debida y oportuna respuesta a las peticiones, así como retenerlas o enviarlas a un destinatario que no corresponde.

    - Ocasionar daño o dar lugar a la pérdida de expedientes, documentos o archivos que hayan llegado a su poder por razón de sus funciones/actividades.

    - Dar lugar al acceso o exhibir expedientes, documentos, información o archivos a personas no autorizadas.

- Realizar actividades tales como borrar, alterar o eliminar información del DPS de manera malintencionada.

VII. Política de Gestión de Medios de Almacenamiento

Objetivo: Proteger la información del DPS que se encuentra en unidades de almacenamiento evitando posibles afectaciones a su confidencialidad, integridad y disponibilidad.

Gestión de medios removibles

1. Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, IPod's, cámaras fotográficas, cámaras de video, celulares, entre otros, estarán controlados en cuanto a su acceso y uso como medio de almacenamiento.

2. La información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles, debe cumplir con las disposiciones de seguridad indicadas por el Grupo de Trabajo de Infraestructura y Soporte de TI (Ver Guía de Clasificación y Etiquetado de la Información), específicamente aquellas referentes al empleo de técnicas de cifrado.

3. El Grupo de Trabajo de Infraestructura y Soporte de TI puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad del DPS o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción conducente a evitar la fuga de información del DPS por medio de medios removibles.

4. Los medios de almacenamiento removibles que se conecten a los equipos de cómputo que sean propiedad del DPS o que estén bajo su custodia, pueden estar sujetos a monitoreo por parte del Grupo de Trabajo de Infraestructura y Soporte de TI.

5. El retiro de medios de almacenamiento de las instalaciones del DPS, tales como discos duros externos, está sujeto a la aprobación del propietario del proceso misional, estratégico o de apoyo, definidos de acuerdo al mapa de procesos del DPS.

6. Todos los medios de almacenamiento removibles deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante. Adicionalmente, se debe hacer seguimiento al deterioro que sufren los medios de almacenamiento para garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible.

Borrado seguro

1. Cuando se borre información de las estaciones de trabajo, se deberá limpiar o vaciar la papelera de reciclaje del sistema.

2. Los medios de almacenamiento que sean de propiedad de terceros, que contengan información del DPS, y que salgan de la Entidad porque ya no se les dará uso, deben seguir un proceso de borrado seguro que garantice que la información del DPS no sea recuperable. (Ver Instructivo de Borrado Seguro de la Información). Este es el caso para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, discos duros externos, etc.

3. Los medios de almacenamiento que contengan información del DPS y que vayan a ser dados de baja o reutilizados, deben seguir un proceso de borrado seguro que garantice que la información del DPS no sea recuperable. (Ver Instructivo de Borrado Seguro de la Información). Este es el caso para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados.

4. Se debe eliminar de forma segura (destrucción, borrado) los medios de almacenamiento que no se utilicen y que contengan información de la Entidad. (Ver Instructivo de Borrado Seguro de la Información).

Medios Físicos en Tránsito

1. La información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles y estos sean transportados fuera de las instalaciones del DPS, debe cumplir con las disposiciones de seguridad indicadas por el Grupo de Trabajo de Infraestructura y Soporte de TI (Ver Guía de Clasificación y Etiquetado de la Información), específicamente aquellas referentes al empleo de técnicas de cifrado.

2. En el caso de que los medios físicos se transporten utilizando los servicios de una empresa transportadora, se deben tomar las precauciones necesarias para garantizar que los medios de almacenamiento sean transportados con precaución para evitar una afectación a la integridad y usabilidad del medio de almacenamiento y asegurar que se identifica adecuadamente al funcionario de la empresa transportadora responsable de la recepción y/o entrega del medio de almacenamiento.

Control de Acceso

I. Política de Control de Acceso

Objetivo: Definir las pautas generales para asegurar un acceso controlado a la información, las aplicaciones y las redes del DPS, así como el uso de medios de computación móvil.

Control de Acceso a Redes y Servicios en Red

1. El DPS suministra a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

2. Solo personal designado por el Grupo de Trabajo de Infraestructura y Soporte de TI está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones del DPS.

3. Todo trabajo que requiera acceder a los servidores, equipos o a las redes del DPS, se debe realizar en las instalaciones. No se podrá realizar ninguna actividad de tipo remoto sin la debida autorización del Grupo de Infraestructura y Soporte de TI.

4. La conexión remota a la red de área local del DPS debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser autorizada por el Grupo de Trabajo de Infraestructura y Soporte de TI, registrada y auditada.

5. La creación y revocación de usuarios en sistemas de información en producción debe seguir un procedimiento formal que garantice la trazabilidad de la operación, y el acceso justificado en una necesidad. (Ver Procedimiento de Creación y Cancelación de Cuentas de Usuario).

Gestión de Contraseñas para usuarios

1. Los usuarios deben acatar las políticas para el uso y selección de las contraseñas de acceso y por lo tanto son responsables de cualquier acción que se realice utilizando el usuario y contraseña de usuario que le sean asignados.

2. Las contraseñas son de uso personal y por ningún motivo se deberán prestar o compartir a otros usuarios.

3. Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

4. Las contraseñas no se deben escribir en ningún medio.

5. Reportar al correo **seguridaddelainformacion@dps.gov.co** sobre cualquier sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

6. Reportar al correo **seguridaddelainformacion@dps.gov.co** sobre cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.

7. Las contraseñas se deberán cambiar según los requerimientos establecidos por el Grupo de Trabajo de Infraestructura y Soporte de TI.

8. Los usuarios deberán cambiar las contraseñas la primera vez que usen las cuentas asignadas.

9. Las contraseñas estarán compuestas al menos por: una letra mayúscula, números o caracteres especiales y su longitud debe ser de mínimo ocho (8) caracteres.

Revisión de los derechos de acceso de los Usuarios

1. Los derechos de acceso de los usuarios a la información y a la infraestructura de procesamiento de información del DPS, deberán ser revisados periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.

Retiro de los derechos de acceso

1. Cada uno de los procesos de la Entidad serán los encargados de comunicar a la Subdirección de Talento Humano, el cambio de cargo, funciones/actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. La Subdirección de Talento Humano será la encargada de comunicar al Grupo de Trabajo de Infraestructura y Soporte de TI sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

Criptografía

II. Política de Uso de Controles Criptográficos

Objetivo: Proteger en confidencialidad, integridad y disponibilidad la información del DPS por medio de técnicas criptográficas apropiadas.

1. Se contemplará la evaluación e implementación de controles criptográficos en la medida que un determinado servicio de procesamiento de información o acceso lo requiera. Se verificarán los medios y herramientas criptográficas que mejor se acoplen a las necesidades de la entidad.

2. Antes de la implementación del tipo de control criptográfico seleccionado, se debe definir y comunicar el procedimiento para la gestión de las llaves públicas o privadas, según el caso, entre las partes interesadas.

3. Las características de los controles criptográficos, incluyendo el tipo, fortaleza y calidad, al igual que las herramientas y mecanismos a emplear para implementar los controles, serán definidos por el Grupo de Trabajo de Infraestructura y Soporte de TI en función de la clasificación de la información. (Ver Guía de Clasificación y Etiquetado de la Información).

4. Se debe garantizar que el uso de controles criptográficos no entorpezca aquellos controles de seguridad basados en inspección de contenido, tales como filtrado web, antimalware, antispyware, etc. El Grupo de Trabajo de Infraestructura y Soporte de TI deberá validar dicha condición y determinar las mejores condiciones de aplicabilidad de los controles criptográficos.

5. Los sistemas de información misionales que involucren accesos desde internet y que gestionen información de criticidad media o alta de acuerdo al inventario de activos de información, deben estar protegidos por un control de cifrado que garantice la confidencialidad, el no repudio y la integridad de los datos, por ejemplo certificados digitales con claves públicas RSA.

6. Para los procesos de cifrado y des cifrado de información se pueden utilizar las recomendaciones y lineamientos definidos en el documento Instructivo de Cifrado y Descifrado de Información, el cual indica los pasos a seguir para generar un archivo cifrado y calcular su posterior código Hash.

Seguridad Física y del Entorno

I. Política de Seguridad Física y del Entorno

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que generen afectaciones a la confidencialidad, integridad o disponibilidad de la información del DPS.

Perímetro de Seguridad Física

1. Todos los ingresos que utilizan sistemas de control de acceso deben permanecer cerrados y es responsabilidad de todos los Colaboradores autorizados evitar que las puertas se dejen abiertas.

2. Se deberá exigir a todos los visitantes, sin excepción, el porte de la tarjeta de identificación de visitante o escarapela en un lugar visible. Así mismo, todos los Colaboradores deberán portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones del DPS.

3. Los visitantes deberán permanecer acompañados de un Colaborador del DPS, cuando se encuentren en las oficinas o áreas donde se maneje información.

4. Es responsabilidad de todos los Colaboradores del DPS borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deberán dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

5. Los visitantes que requieran permanecer en las oficinas del DPS por periodos superiores a dos (2) días deberán ser presentados al personal de oficina donde permanecerán.

6. El horario autorizado para recibir visitantes en las instalaciones del DPS es de 8:15 AM a 5:15 PM. En horarios distintos se requerirá de la autorización del Director, Jefe de Oficina, Subdirector o Coordinador del Grupo correspondiente.

7. Los equipos portátiles, así como toda información CONFIDENCIAL del DPS, independientemente del medio en que se encuentre, deberán permanecer guardados bajo llave durante la noche o en horarios en los cuales el Colaborador responsable no se encuentre en su sitio de trabajo.

8. Las instalaciones del DPS en el Nivel Nacional deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de Colaboradores, terceros y visitantes.

Controles de Acceso Físico.

1. Las áreas seguras, dentro de las cuales se encuentran el Centro de Cómputo, centros de cableado, áreas de archivo y áreas de recepción y entrega de correspondencia, deberán contar con mecanismos de protección física y ambiental, y controles de acceso que pueden ser mediante tarjeta de proximidad o puertas con cerradura.

2. En las áreas seguras, bajo ninguna circunstancia se podrá fumar, comer o beber.

3. Las actividades de limpieza en las áreas seguras deberán ser controladas y supervisadas por un Colaborador del proceso. El personal de limpieza deberá ser instruido acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohibirá el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

Ubicación y Protección de los equipos.

1. La infraestructura tecnológica (Hardware, software y comunicaciones) deberá contar con medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

2. Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Seguridad de los equipos fuera de las instalaciones

1. Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deberán ser controlados mediante el cifrado de la información almacenada en sus discos duros, utilizando la herramienta definida por el Grupo de Trabajo de Infraestructura y Soporte de TI.

2. Los equipos portátiles no deberán dejarse a la vista en el interior de los vehículos. En casos de viaje siempre se deberán llevar como equipaje de mano.
3. En caso de pérdida o robo de un equipo portátil se deberá informar inmediatamente a la Subdirección de Operaciones y se deberá poner la denuncia ante la autoridad competente y allegar copia de la misma.

4. Los equipos portátiles deben estar asegurados (cuando los equipos estén desatendidos) con una guaya, dentro o fuera de las instalaciones del DPS.

5. Los puertos de transmisión y recepción de infrarrojo y "*Bluetooth*" deberán estar deshabilitados.

6. Cuando un equipo de cómputo deba retirarse de las instalaciones del DPS se deberá utilizar el formato y procedimiento correspondiente.

Seguridad en la reutilización o eliminación de los equipos

1. Cuando un equipo de cómputo sea reasignado o dado de baja, se deberá realizar una copia de respaldo de la información que se encuentre almacenada. Luego el equipo deberá ser sometido a un proceso de eliminación segura de la información almacenada y del software

instalado, con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma. (Ver Procedimiento de Borrado Seguro).

Retiro de Activos

1. Los equipos de cómputo, la información o el software no deben ser retirados de la Entidad sin una autorización formal. Periódicamente se deben llevar a cabo por parte de la Subdirección de operaciones, comprobaciones puntuales para detectar el retiro no autorizado de activos de la Entidad.

II. Política de escritorio despejado y pantalla despejada

Objetivo: Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información del DPS durante y fuera del horario de trabajo normal de los usuarios.

1. El personal del DPS debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

2. El personal del DPS debe bloquear la pantalla de su computador con el protector de pantalla designado por la Entidad, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo. Al finalizar sus actividades diarias, deberán salir de todas las aplicaciones y apagar la estación de trabajo.

3. Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deberá reutilizar papel que contenga información CONFIDENCIAL.

4. En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar la información CONFIDENCIAL protegida bajo llave. Esto incluye: documentos impresos, CD´s, dispositivos de almacenamiento USB y medios removibles en general.

SEGURIDAD DE LAS OPERACIONES

I. Política de Gestión de Cambios

Objetivo: Asegurar que los cambios de alto impacto realizados sobre la organización, los procesos de negocio, las instalaciones o los sistemas de procesamiento de información se realicen de forma controlada.

1. Toda solicitud de cambio en los servicios de procesamiento de información, se debe realizar siguiendo el Procedimiento de gestión de cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información, e igualmente tener una trazabilidad de este tipo de solicitudes. El procedimiento de gestión de cambios especifica los siguientes canales autorizados para la recepción de solicitudes de cambios: Mesa de Ayuda o Helpdesk, correo electrónico o memorando dirigidos al Coordinador de GT Infraestructura y Soporte de TI

2. Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, bien sea porque se trate de actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad del aplicativo o a los componentes que soportan el sistema de información, tales como el sistema operativo o cambios en hardware. Existe sin embargo una situación especial para cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada. (Ver Procedimiento de gestión de cambios)

3. Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los Colaboradores que por sus funciones tienen relación con el sistema de información.
4. Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información. Estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

5. Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantienen las condiciones de operatividad del sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema, y que el propósito del cambio se cumplió satisfactoriamente.

6. Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

II. Política de Gestión de la capacidad

Objetivo: Asegurar la disponibilidad de los recursos necesarios para la operatividad de los sistemas de información contemplando necesidades actuales y futuras

1. El Grupo de Trabajo de Infraestructura y Soporte de TI definirá las actividades específicas para monitorear, proyectar y asegurar la capacidad de la infraestructura de procesamiento de información, con el objeto de garantizar el buen desempeño de los recursos tecnológicos necesarios para la ejecución de los procesos.

2. La capacidad de los recursos debe ser ajustada periódicamente para garantizar la disponibilidad y eficiencia requerida de acuerdo a las necesidades actuales y futuras del DPS.

3. El monitoreo y gestión de la capacidad debe hacerse considerando la criticidad de la información y los sistemas que soportan, para lo cual se utilizará la criticidad determinada durante el levantamiento del inventario de activos de información. Aquellos componentes que soporten activos con criticidad alta siempre deben estar sujetos a monitoreo y gestión de capacidad.

4. Se debe tomar las acciones adecuadas para minimizar o evitar la dependencia de elementos o personas claves para la prestación de un servicio. Dentro de las acciones se deben contemplar: redundancia de elementos, arquitecturas de contingencia o de alta disponibilidad, técnicas de gestión de conocimiento sobre la operatividad de la infraestructura, etc.

5. Los umbrales de óptimos de capacidad se puede obtener incrementando la capacidad o reduciendo la demanda, lo cual incluye las siguientes posibles acciones que deberán ser llevadas a cabo por el Grupo de Trabajo de Infraestructura y Soporte de TI: Eliminación de información obsoleta, supresión de aplicaciones, bases de datos o ambientes en desuso, optimización de procesos o tareas automáticas, afinamiento de consultas a bases de datos o lógica de aplicaciones, restricción de ancho de banda para servicios con alto consumo de capacidad que no sean misionales, etc.

III. Política de paso de ambientes de desarrollo, pruebas y producción

Objetivo: Reducir riesgos asociados a modificaciones, cambios o accesos no autorizados en sistemas en producción del DPS

1. Se deben establecer y mantener ambientes separados de Desarrollo, Pruebas y Producción, dentro de la infraestructura de Desarrollo de Sistemas de Información del DPS. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario de activos de información.

2. El ambiente de desarrollo se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código. Por su parte, el ambiente de pruebas se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas hacia el software teniendo como base los criterios de aceptación y los requerimientos de desarrollo. Finalmente, el ambiente de producción debe utilizarse para la prestación de un servicio que involucra la manipulación de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la entidad.

3. Se debe seguir un procedimiento formal para el paso de software y aplicaciones de un ambiente a otro (desarrollo, pruebas y producción), que establezca las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a uno existente. Esto aplica para sistemas que contengan información catalogada con criticidad alta de acuerdo al inventario de activos de información. (Ver Procedimiento de paso de ambientes de desarrollo, pruebas y producción).

4. No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.

5. En los ambientes de desarrollo y pruebas no se deberán utilizar datos reales del ambiente de producción, si antes haber pasado por un proceso de ofuscamiento (Ver Procedimiento de Ofuscamiento de Datos).

6. Se debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.

7. Se deben utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

8. Cada uno de los ambientes deben estar claramente identificados, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada ambiente.

9. Los cambios a sistemas en producción que involucren aspectos funcionales deben ser informados y consultados con el(los) proceso (s) propietario(s) de la información.

10. Se debe acoger lo establecido en el Documento Guía de Desarrollo de Software para el DPS.

IV. Política de Protección contra Código Malicioso

Objetivo: Establecer medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos.

1. Toda la infraestructura de procesamiento de información debe contar con un sistema de detección/prevención de intrusos, sistema anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores del DPS.

2. Se restringirá la ejecución de código móvil aplicando políticas en el sistema operacional, en el software de navegación de cada máquina y en el sistema de control de navegación.

3. Los usuarios de los servicios TIC del DPS son responsables de la utilización de programas antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos y/o removibles y/o los archivos y/o el correo electrónico que esté autorizado a emplear.

4. El DPS contará permanentemente con los programas antivirus de protección a nivel de red y de estaciones de trabajo, contra virus y/o código malicioso, el servicio será administrado por el Grupo de Trabajo de Infraestructura y Soporte de TI.

5. Los programas antivirus deben ser instalados por el Grupo de Trabajo de Infraestructura y Soporte de TI en los equipos centralizados de procesamiento y en las estaciones de trabajo de modo residente para que estén activados durante su uso. Las instalaciones nuevas de estaciones de trabajo o servidores que sirvan al propósito operativo del DPS deben contar con un programa de antivirus previo a la instalación de cualquier otro programa sobre el sistema operativo.

6. Los servicios de TIC que se emplean para servir a una finalidad operativa y administrativa en

relación con la entidad y que intercambien información o los sistemas que la procesan, redes y demás infraestructura TIC del DPS se consideran bajo el control de la entidad y pueden ser revisados por el administrador de la suite de productos de seguridad.

7. Se debe actualizar periódicamente las versiones de los componentes de los diferentes sistemas de seguridad operativos, incluidos, motores de detección, bases de datos de firmas, software de gestión en el lado cliente y servidor, etc.

8. Se debe validar de forma periódica el uso de software no malicioso en las estaciones de trabajo y servidores. Esta labor se debe programar de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo del Grupo de Trabajo de Infraestructura y Soporte de TI.

9. Se deben tener controles para analizar, detectar y restringir el software malicioso que provenga de posibles fuentes de código malicioso, entre ellas: descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

10. Se deben generar boletines informativos acerca de las formas de reconocer malware, hoax, spyware, etc., los cuales ayuden a generar una cultura de seguridad de la información entre los Colaboradores del DPS.

11. Los Colaboradores del DPS pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Colaboradores siempre podrán consultar al Grupo de Trabajo de Infraestructura y Soporte de TI sobre el tratamiento que debe darse en caso de sospecha de malware.

12. Los Colaboradores no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus y/o de detección de código malicioso, en los equipos o sistemas en que estén instalados.

13. Todo usuario es responsable por la destrucción de todo archivo o mensaje, que le haya sido enviado por cualquier medio provisto por el DPS, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta **seguridaddelainformacion@dps.gov.co** con la frase “correo sospechoso” en el asunto.

14. El único servicio de antivirus autorizado en la entidad es el asignado directamente por el Grupo de Trabajo de Infraestructura y Soporte de TI, el cual cumple con todos los

requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por el Grupo de Trabajo de Infraestructura y Soporte de TI, a efectos de reforzar el control de presencia y/o programación de virus y/o código malicioso.

15. El Grupo de Trabajo de Infraestructura y Soporte de TI es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los computadores y/o equipos informáticos de la red del DPS que son empleados por los Colaboradores que desempeñen labores/actividades en la Entidad.

16. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, tramitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

17. El Grupo de Trabajo de Infraestructura y Soporte de TI se reserva el derecho de filtrar los contenidos que se trasmitan en la red del DPS para evitar amenazas de virus. Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

V. Política de Backup

Objetivo: Proporcionar medios de respaldo adecuados para asegurar que la información esencial y el software asociado se pueda recuperar después de una falla.

1. La información de cada sistema de información debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, CD, DVD, de acuerdo a su nivel de criticidad identificada en el inventario de activos de información. La información con criticidad mayor debe estar sujeta a una mayor frecuencia de tareas de respaldo. Los medios se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico (Ver Procedimiento de Ejecución de Backups).

2. Se deben realizar pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad (Ver Procedimiento de Restauración de Backups).

3. El Custodio de cada activo de información es el responsable de verificar que los backups se ejecuten correctamente y de acuerdo al tipo y frecuencia acordados.

4. El administrador de las Bases de Datos y el Oficial de Seguridad de la Información son los responsables de definir la frecuencia de respaldo, el tipo, el medio de almacenamiento y los requerimientos de seguridad de la información, de acuerdo a las disposiciones definidas en la Guía de Clasificación y Etiquetado de la Información. Estos aspectos de configuración se deben registrar en el Formato de Definición de Backups de Información

5. Todas las copias de información con criticidad alta deben ser almacenadas en un área adecuada y con control de acceso.

6. Las copias de respaldo se deben guardar con el objetivo de restaurar el sistema luego de una infección de virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, contaminación de los datos y por requerimientos legales.

7. Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

8. Es responsabilidad de cada Colaborador ubicar la información más crítica asociada con su labor encomendada en el servidor de archivos definido para cada usuario. El servidor de archivos estará protegido con un sistema de respaldo de la información.

VI. Política de Auditoria

Objetivo: Asegurar el registro de los eventos y las operaciones realizadas sobre los sistemas de información del DPS que permita contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

Registro de eventos

1. Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones del DPS, deben ser registrados. Para ello se debe habilitar los log de eventos requeridos y deben ser revisados con regularidad.

2. La información generada por los logs o eventos monitoreados, se deben proteger y guardar evitando el acceso o manipulación no autorizada.

Registro del administrador y del Operador

1. Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información del DPS deberán estar debidamente registradas.

2. Los administradores de la infraestructura de procesamiento de información tendrán asignada una cuenta de usuario única, a través de la cual se realizarán las actividades de administración.

Sincronización de relojes

1. Todos los relojes de la infraestructura de procesamiento de información del DPS, deberán estar sincronizados con la hora legal Colombiana.

VII. Política de Gestión de vulnerabilidades técnicas.

Objetivo: Gestionar las vulnerabilidades técnicas asociadas a la plataforma tecnológica del DPS para reducir la posibilidad de existencia de amenazas informáticas.

1. El Grupo de Trabajo de Infraestructura y Soporte de TI, se encargará de identificar las vulnerabilidades técnicas de la plataforma tecnológica. Para ello, La gestión de vulnerabilidades técnicas estará basada en diferentes estrategias:

   - Monitoreo sobre la plataforma tecnológica.
   - Reportes de fabricantes y proveedores.
   - Servicios de seguridad informática contratados.
   - Reportes de usuarios internos y externos.

2. Las contramedidas a implementar para minimizar el riesgo ante el hallazgo de vulnerabilidades técnicas, serán comunicadas a cada uno de los custodios de los activos de información al igual que su implementación o tratamiento.

SEGURIDAD DE LAS COMUNICACIONES

I. Política de Gestión de Seguridad de las Redes

Objetivo: Definir los controles necesarios para proteger la información del DPS transportada a través de la red interna y a través de la red de conexión hacia terceros

1. Se establecerá un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad establecidos.

2. El DPS proporciona a los Colaboradores todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones/actividades para las cuales fueron contratados, por tal motivo no se permite conectar a las estaciones de trabajo o a los puntos de acceso corporativos, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el Grupo de Trabajo de Infraestructura y Soporte de TI.

3. El acceso remoto a la red de datos del DPS se permitirá de acuerdo a la Política de Teletrabajo.

Separación de las Redes

1. Se debe establecer un esquema de segregación de redes con el fin de controlar el acceso a los diferentes segmentos de red. El tráfico entre estos segmentos de red estará controlado mediante un elemento de red que permita una autorización a un nivel de detalle específico (Dirección IP, puerto).

II. Política de Transferencia de información

Objetivo: Proteger la información del DPS que es intercambiada o transferida en razón de las actividades propias de la Entidad

Acuerdos para el Intercambio de información

1. Se debe firmar Acuerdos de Confidencialidad con Colaboradores y terceros que por diferentes razones requieran conocer o intercambiar información no PUBLICA que se encuentre en custodia del DPS. En estos acuerdos deben quedar especificadas las responsabilidades para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información. (Ver Acuerdo de Confidencialidad Individual y Acuerdo de Confidencialidad con terceros).

2. Se debe considerar la normatividad aplicable para el intercambio de información no PÚBLICA con terceros. Específicamente se debe considerar el mecanismo, por ejemplo: Convenios Interadministrativos, definido por la Oficina Asesora Jurídica para formalizar los intercambios de información.

3. Todos los Colaboradores deben firmar el Formato “Acuerdo individual de Manejo de la Información” definido por el DPS y este debe ser parte integral de cada uno de los contratos o de la carpeta de documentos de posesión de los funcionarios.

4. El encargado de asegurar el trámite de firma, custodia y mantenimiento de los acuerdos, será la Subdirección de Talento Humano.

5. Este requerimiento también se aplica para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la institución a personas o entidades externas.

6. Los formatos de Acuerdos de Confidencialidad, serán revisados y aprobados por el Grupo de Infraestructura y Soporte de TI.

7. Las entregas y transferencias de información asociada a los programas de la Entidad se resolverán de acuerdo al Procedimiento de entrega de bases de datos. Adicionalmente, en caso de que se requiera un proceso de cifrado y des cifrado de información (Por ejemplo para información Reservada y Confidencial, tal como lo define la Guía de clasificación y etiquetado de la información) se pueden utilizar las recomendaciones y lineamientos definidos en el documento Instructivo de Cifrado y Descifrado de Información, el cual indica los pasos a seguir para generar un archivo cifrado y calcular su posterior código Hash.

ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

I. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Objetivo: Considerar la seguridad de la información como un componente transversal en la totalidad del ciclo de desarrollo de sistemas de información

Requisitos de seguridad de los sistemas de información

1. La construcción y modificación de sistemas de información o la implementación de nuevos módulos a los sistemas de información misionales o de apoyo, desarrollados al interior de la entidad o contratados con terceras partes, deben contemplar un completo análisis de requerimientos en cuanto a seguridad de la información, análisis de riesgos y posibles escenarios de riesgos asociando los controles respectivos para la mitigación de los mismos.

2. Todas las solicitudes para compra, actualización y/o desarrollo de software deberán ser direccionadas, orientadas, con el acompañamiento y bajo los estándares definidos por el Grupo de Trabajo de Infraestructura y Soporte de TI.

3. Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

4. Únicamente está permitido el uso de software autorizado por el Grupo de Trabajo de Infraestructura y Soporte de TI. Para ambientes de Desarrollo se debe utilizar el estándar adoptado por la Entidad que es .NET, así como la plataforma para Bases de Datos que es Oracle y SQL server.

5. Para todo esto, se debe acoger lo establecido en el Documento Guía de Desarrollo de Software para el DPS.

6. El acceso de los usuarios a los sistemas de información misionales y de apoyo se restringirá mediante autenticación por usuario y clave de acceso, para cada usuario se delimitaran los perfiles de acceso y procesamiento de información según las necesidades. La definición de los tipos de perfiles será determinada por los administradores de los sistemas de información de cada uno de los procesos.

Procedimientos de control de cambios

1. Cualquier tipo de cambio sobre los sistemas de información deberá seguir lo establecido el Documento Guía de Desarrollo de Software para el DPSy tener en cuenta la aceptación de las pruebas técnicas y funcionales dictaminadas por cada uno de los responsables a quienes afectaran los cambios que se realicen.

Desarrollo de software contratado externamente

1. El desarrollo de software contratado con terceras partes, deberá contemplar todos los requisitos en cuanto a seguridad de la información fijados en este documento, solo se darán por recibidos desarrollos realizados sobre los estándares de la entidad en cuanto a herramienta de desarrollo, y pruebas técnicas y funcionales.

2. Los contratos de desarrollo de software con terceros deberán tener claramente definidos los alcances de las licencias, los derechos de propiedad del código desarrollado y los derechos de propiedad intelectual, junto con los requerimientos contractuales relacionados con la calidad y seguridad del código desarrollado.

3. Se debe realizar un análisis de vulnerabilidades técnicas a los sistemas de información desarrollados y que estén en proceso de paso a producción, para garantizar que los nuevos desarrollos no exponen la seguridad de la información del DPS ni su infraestructura. Esta actividad está a cargo del Grupo de Trabajo de Infraestructura y Soporte de TI.

RELACIÓN CON LOS PROVEEDORES

I. Política de Seguridad de la Información para las Relaciones con los Proveedores

Objetivos: Proteger en términos de seguridad la información del DPS accedida por los proveedores

Consideraciones de seguridad en los acuerdos con terceras partes

1. En los Contratos o Acuerdos con terceras partes y que implique un intercambio, uso o procesamiento de información de la Entidad, se debe contemplar la posibilidad de celebrar Acuerdos de Confidencialidad en el manejo de la información. Estos acuerdos deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio. El contrato o acuerdo debe definir claramente el tipo de información que intercambiaran las partes.

GESTION DE INCIDENTES

I. Política de Gestión de Incidentes de Seguridad de la Información

Objetivo: Gestionar adecuadamente los incidentes de seguridad de la información presentados en el contexto del DPS

Reporte sobre los eventos y las debilidades de la seguridad de la información

1. Es responsabilidad de cada uno de los Colaboradores de la entidad y terceras partes, reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información; esto con el fin de proceder con el tratamiento respectivo. (Ver Procedimiento de Notificación de Eventos y Gestión de Incidentes de Seguridad de la Información).

Gestión de los incidentes y mejoras en la seguridad de la información

1. A todos los incidentes de seguridad reportados, se les debe dar el tratamiento y seguimiento respectivo, realizando el respectivo trámite ante las instancias correspondientes. (Ver Procedimiento de Notificación de Eventos y Gestión de Incidentes de Seguridad de la Información).

ASPECTOS DE SEGURIDAD PARA LA GESTION DE CONTINUIDAD DE NEGOCIOS

I. Política de Gestión de la Continuidad del Negocio

Objetivo: Garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información del DPS

Seguridad de la información en la continuidad del negocio

1. Ante la ocurrencia de eventos no previstos en cuanto a la indisponibilidad del Centro de Datos principal, el DPS debe contar y asegurar la implementación de un Plan de Recuperación de Desastres que asegure la continuidad de las operaciones tecnológicas de sus procesos críticos.

2. Para el DPS su recurso más importante es el *Recurso Humano* y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier situación.

3. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, deben estar incorporados y definidos en un “Plan de contingencias”.

Pruebas y mantenimiento del plan de continuidad del negocio

1. Se debe establecer un plan de pruebas periódico del plan de Contingencia de la Plataforma Tecnológica del DPS.

CUMPLIMIENTO DE LOS REQUISITOS LEGALES

I. Política de Cumplimiento Legal

Objetivo: Garantizar el cumplimiento de los requisitos legales a los cuales está sometido el DPS en función de la información que custodia

Identificación de la Legislación Aplicable

1. EL DPS debe cumplir con todos los requisitos de la legislación aplicable propia de las leyes colombianas, las derivadas del sector social y las obligaciones contractuales con proveedores, contratistas y terceros. (Ver Matriz de Legislación Aplicable).

2. El Grupo de Trabajo de Infraestructura y Soporte de TI debe mantener el control de todas las licencias de software y aplicaciones utilizadas en el DPS.

3. Se deben realizar revisiones periódicas a los sistemas de información y estaciones de trabajo, a fin de verificar el cumplimiento con el software autorizado.

4. Está prohibido el uso de software ilegal no autorizado en sus estaciones de trabajo.

Derechos de propiedad intelectual

1. No se permite el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal, y con la autorización del DPS.

2. Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

Protección de los registros de la Organización

1. Todos los registros del DPS, independientemente del medio de almacenamiento en el que se encuentren, deberán ser protegidos contra pérdida, destrucción y falsificación.

2. La información contenida en las estaciones de trabajo propiedad del DPS, son de propiedad de la Entidad.

3. No se permitirá el almacenamiento y/o procesamiento de información de propiedad del DPS en equipos o dispositivos de propiedad de los Colaboradores.

Anexo D. Política de backups

Copias de Seguridad y Recuperación

Contenido

INTRODUCCIÓN

El presente documento corresponde al aparte del diseño de Windows 2008 y Exchange 2010 Server para el departamento Administrativo para la Prosperidad Social, en cuanto a Copias de Seguridad y Recuperación.

Los capítulos que conforman este documento corresponden al esquema de copias de respaldo que posee el DPS en sus actuales servidores y servicios que corren sobre estos.

OBJETIVOS

Objetivo General

Se tiene un esquema de copias de seguridad de los servicios y Bases de Datos del DPS, que vayan de la mano con el Plan de contingencia para evitar un posible desastre que llegase a ocurrir y que da alguna manera el DPS pueda recuperase a tal eventualidad.

Objetivos Específicos

- Diseñar el esquema de backups que debe poseer el DPS.
- Explicar cómo funciona el esquema de backups dentro del DPS.
- Explicar los diferentes backups que se dan al interior del DPS.
- Explicar a qué se le debe realizar respaldo.
- Cómo funciona el esquema de respaldos y de custodia.

Copias de Seguridad y Recuperación en Desastres – Plan de Contingencia

Plan de Copias de Seguridad

Se contará con las siguientes estrategias de copias de seguridad dependiendo de la función que realice cada uno de los servidores miembros del dominio del DPS**.**

Plan y Estrategia de copias de Seguridad

La estrategia de Copias de Seguridad, es definitivamente la clave en materia de protección de la información, y en Windows 2008 no es la excepción. En esta sección se describirá la estrategia de Copias de Seguridad propuesta para la infraestructura de Windows 2008**.**

Herramientas de Backup

Windows 2008 provee una herramienta de backup que permite proteger los datos de una perdida accidental o de una falla en el hardware o almacenamiento. Usando la herramienta de backup que viene con el sistema operativo se puede crear una copia duplicada de los datos en el disco duro y archivar los datos en otro dispositivo de almacenamiento como un disco duro o una unidad de cinta.

Con el asistente del Backup se puede:

- Crear una copia de archivo de los archivos seleccionados y carpetas en un disco duro.
- Agendar un backup regular.
- Restaurar las carpetas y archivos almacenados para el disco o cualquier otro disco que pueda acceder.
- Respaldar el Directorio Activo.
- Respaldo offline de datos almacenados remotamente.

Al igual se va utilizar una herramienta diferente a la que viene con el sistema operativo, esta herramienta es **HP OpenView Storage Data Protector**. Esta herramienta se utiliza con el fin de realizar backups a los archivos de usuarios que se encuentra sobre el servidor Calipso, con esta herramienta también se puede hacer backup a los buzones de correo de los usuarios y las Bases de Datos Oracle y SQL Server.

Estrategias de Backup

Una buena estrategia de backup es la mejor defensa contra la perdida de datos. Las tres estrategias comunes de backup son las siguientes:

- **Backup de Red o Servidor Únicamente:** Se planea respaldar toda la red, o se tienen dispositivos de almacenamiento a ciertos servidores donde los usuarios guardan su información importante.

- **Backup Individual o al Computador Local:** Cada computador necesita un dispositivo de almacenamiento. Cada usuario es responsable por el respaldo de sus datos.

- **Backup del Servidor y Computador:** Cada departamento tiene un dispositivo de almacenamiento y un usuario designado para respaldar toda la información del departamento.

Para el caso del DPS donde la estructura de la red y la administración es centralizada, se recomienda un Backup a los servidores, donde se encuentre la información importante tanto de la organización como de los usuarios. La información que no esté sobre los servidores designado y/o que estén en estaciones es responsabilidad de cada funcionario o área.

Consideraciones al Plan de Backup

Cuando se desarrolla un plan de backup se debe tener en cuenta:

- Estar seguro de que se tiene un separado hardware en el caso de que falle un dispositivo de backup.
- Probar los datos del backup regularmente para verificar la fiabilidad del procedimiento de backup y del equipo.
- Incluir una prueba de tensión del hardware de backup (unidades de almacenamiento, unidades ópticas y controles) y del software (programas de backup y unidades de dispositivo).

Para el caso del DPS se cuenta con una librería marca HP StorageWorks MSL 2024 G3 Series, que cuenta con dos unidades de tape de 800/1600 GB de almacenamiento cada una de las cintas.

Tipos de Backup

Los backups en Windows 2008, se pueden dividir en varios tipos; tanto con la herramienta de Windows como HP OpenView Storage Data Protector, como son los siguientes:

- Un Bac*kup Normal* copia todos los archivos seleccionados y marca cada uno como un backup normal. Para la restauración es solamente necesario el más reciente backup realizado.

- Un *Backup Incremental*, realiza backup solamente a los archivos que fueron creados o modificados desde el último backup normal o incremental. Este marca solamente los archivos que se les ha realizado backup. Al utilizar una combinación de backups normales e increméntales es necesario para la restauración tener el último backup normal y todo el set de backups increméntales hasta la fecha.

- Un *Backup Diferencial*, copia los archivos creados o modificados desde el último backup normal o incremental. Este no marca los archivos como si se le hubiera realizado backup. Si se tiene una combinación de backups normales y diferenciales; para la restauración es necesario tener el último backup normal y el set de backups diferenciales.

- Un *Backup Copia*, copia todos los archivos seleccionados, pero no marca los archivos como si se le hubiera hecho backup. Este backup no afecta otros tipos de backup.

- Un *Backup Diario*, copia todos los archivos seleccionados que han sido modificados en el día que se haya realizado el backup. Los archivos no son marcados.

Windows 2008, trae una característica que permite realizar un backup a un archivo. Esto es una gran ventaja cuando sobre los servidores no se tienen unidades de cinta; aunque el backup realizado sigue siendo a cinta. Con la herramienta de Data Protector se posee más flexibilidad con los backups ya que también se puede enviar a cinta, aunque este maneja agentes para los servidores que se le va a hacer backup como si fuese de forma local.

Información que se debe respaldar

- De los controladores de dominio se debe realizar copia del estado del sistema para respaldar el directorio activo.
- De los servidores de archivos se deben respaldar las carpetas compartidas y el estado del sistema.
- De los servidores de Exchange se debe hacer copias de las bases de datos de correo y de carpetas públicas.
- Se deben mantener discos de reparación actualizados por cada servidor y almacenados de manera segura.
- Los servidores que manejan sitios y aplicaciones web.
- Las bases de datos de los servidores Oracle y SQL.

Para obtener información relacionada, consulte en Microsoft Knowledge Base el artículo 216993, "Backup of the Active Directory Has 60-Day UsefulLife" (**http://go.microsoft.com/fwlink/?LinkId=3052&kbid=216993**) (este artículo está en inglés).

Backup de datos del SystemState Controladores de Dominio, Archivos, Correo y Bases de Datos

El SystemState es la configuración del sistema; este varía dependiendo del rol de la maquina Windows 2008 (si es DC, Cluster entre otros). Es muy importante el backup del SystemState, ya que sobre él se encuentra la configuración de los servidores y estaciones.

Los datos del SystemState están comprendidos por los siguientes archivos:

- Los archivos Boot, incluyendo los archivos del sistema, y todos los archivos protegidos por Windows File Protection (WFP).
- El Directorio Activo (en un controlador de dominio solamente).
- Sysvol (en un controlador de dominio solamente).
- Servicio de Certificados (en autoridades de certificación solamente).
- Base de datos Cluster (en un nodo del Cluster, solamente donde se encuentre el servicio).
- El registro.
- Información del contador de configuración del desempeño.
- Base de datos de registro de las clases de servicio del Componente.

A Los datos del SystemState se les puede realizar backup en cualquier orden. La restauración del SystemState remplaza los archivos de Boot primero y confía en la carga del registro del sistema como paso final en el proceso.

La operación de Backup y restore del SystemState incluye todos los datos del sistema: No se le puede seleccionar al backup o al restore componentes individuales debido a la dependencia entre los componentes del SystemState. Sin embargo, se puede restaurar los datos del SystemState en una localización alterna en la cual solamente los archivos de registro, el directorio de archivos del Sysvol, y el sistema de archivos de Boot son restaurados.

La base de datos del Directorio Activo, la base de datos del servicio de certificado, y la base de datos de los componentes de servicios de clases registradas no son restauradas en una localización alterna.

Se recomienda hacer una copia de seguridad del SystemState sobre un archivo en el disco duro, para que desde un servidor que tenga unidad de cinta a través de la red se realice el backup a este archivo.

Para obtener más información acerca de estos métodos de copia de seguridad, consulte "Recuperación de desastres" en la Ayuda en pantalla de Windows Server 2003, Standard Edition(**http://go.microsoft.com/fwlink/?LinkId=28311)**

Controladores de dominio

Dada la funcionalidad que tendrá el servidor TITAN y SKOLL como Controladores de Dominio, del sitio principal (Nivel Nacional); se recomienda para proteger el directorio activo, realizar copias de seguridad regulares del "SystemState", adicionalmente antes de instalar un nuevo driver o una nueva aplicación se debe actualizar el disco de reparación de sistema, una vez comprobada la correcta funcionalidad del servidor se debe actualizar nuevamente el disco de reparación.

	SystemState (Controladores de Dominio)
Lunes - Sábado	
Domingo	✓

Las copias de seguridad en el servidor TITAN y SKOLL se deberán realizar de acuerdo a la siguiente plantilla:

Para obtener más información acerca de estos métodos de copia de seguridad, consulte "Recuperación de desastres" en la Ayuda en pantalla de Windows Server 2008,(http://social.technet.microsoft.com/Forums/en-US/5863774c-df6b-457f-bbbd-d7aae1e25615/archivos-necesarios-para-restaurar-win-2008-server-tras-un-desastre**)**

Servidor de Archivos

De igual forma es necesario respaldar la información almacenada en los recursos compartidos, la cual abarca:

- Información importante propia de los usuarios pero relacionada con el trabajo diario en el DPS.
- Información necesaria para el trabajo diario de los usuarios del DPS.

Se recomienda realizar una copia diaria de toda la información almacenada en los recursos compartidos esto para el caso de archivos (Servidor Calipso).

	SystemState (Calipso)	Normal (Calipso)
Lunes		✓
Martes		✓
Miércoles		✓
Jueves		✓
Viernes		
Sábado		✓
Domingo	✓	

Servidor de correo Backend

Dada la funcionalidad que tendrá el servidor JANUS y JANUSS como Servidor de Correo Back End se recomienda para proteger el correo electrónico, realizar copias de seguridad regulares del "systemstate", adicionalmente antes de instalar un nuevo driver o una nueva aplicación se debe actualizar el disco de reparación de sistema, una vez comprobada la correcta funcionalidad del servidor se debe actualizar nuevamente el disco de reparación.

Se recomienda realizar copias de seguridad regulares de las bases de datos de correo tanto Online como Offline (Offline se puede tomar respaldo cada vez que se haga mantenimiento de las bases de datos de Exchange).

Las copias de seguridad en el servidor JANUS y JANUSS se deberán realizar de acuerdo a la siguiente plantilla:

	SystemState	Normal	Online BDs
Lunes		✓	
Martes		✓	

Miércoles		✓	
Jueves		✓	
Viernes			
Sábado		✓	✓
Domingo	✓		

Además es recomendable cada vez que se realicen modificaciones en la configuración de los sitios Web, realizar backup a la Metabase de Internet Information Server y respaldarla en cinta. El archivo generado por el procedimiento de backup de la metabase se almacena en la ruta **C:\WINDOWS\system32\inetsrv\MetaBack.**

*Exchange Server 2010 Disaster Recovery Planning Guide (*http://technet.microsoft.com/en-US/exchange/dd203064.aspx)

Servidor de correo Frontend

Dada la funcionalidad que tendrá el servidor TARVOSS como Servidor Web y Servidor de Correo Front End se recomienda realizar copias de seguridad regulares del "systemstate", adicionalmente antes de instalar un nuevo driver o una nueva aplicación se debe actualizar el disco de reparación de sistema, una vez comprobada la correcta funcionalidad del servidor se debe actualizar nuevamente el disco de reparación.

Con respecto al respaldo de la información de sitios Web se recomienda realizar copias de seguridad regulares y cuando esta cambie.

Las copias de seguridad en el servidor TARVOSS se deberán realizar de acuerdo a la siguiente plantilla:

	SystemState	**Normal**
Lunes - Sábado		
Domingo	✓	

Además es recomendable cada vez que se realicen modificaciones en la configuración de los sitios Web realizar backup a la Metabase de Internet Information Server y respaldarla en cinta. El archivo generado por el procedimiento de backup de la metabase se almacena en la ruta **C:\WINDOWS\system32\inetsrv\MetaBack.**

Bases de Datos

La entidad posee dos motores de Base de Datos que corresponde a Oracle 10g, 11g y SQL Server versión 2005/2008/2012

Se posee un plan de Backups diarios que se generan automáticamente todos los días a partir de las 12:01 a.m. de la mañana.

El Backup se genera en una carpeta creada en el sistema de almacenamiento (HP-EVA 6500), en la cual se crea un archivo con el nombre de los esquemas de la BD y la fecha de cada día, junto con este archivo se genera un log que muestra el resultado de cada Backup.

Proceso de Copia a Cinta

Los Backups generados en el sistema de almacenamiento se llevan a cintas de 800/1600GB, estas cintas son rotuladas con una etiqueta con código de barras que suministra la empresa que resguarda las cintas, además se registra en una planilla la bitácora del proceso de backup.

Plan De Copias De Seguridad para el DPS

La estrategia de backups corresponde a los backups de las Bases de Datos, las aplicaciones, configuración de servidores, archivos de usuarios, archivos de áreas, aplicaciones web, Buzones y Bases de Datos de Correo electrónico; estos backup se hacen a través de la herramienta de HP - Data Protector.

Backup Bases de Datos (Oracle y SQL)

Desde cada sistema de base de datos (Oracle y SQL) se programan a través del Sistema Operativo o la BD una tarea para que realice el backup a disco de forma automática entre las 0 horas y las 4:00 a.m. de la mañana.

Para las Bases de Datos se generan 2 cintas de backup, una se envía a custodia externa y la otra queda en custodia interna, esta se guarda en la caja fuerte del Área de Sistemas.

El administrador verifica los backups y los log (.Dmp en Oracle y .Bak en SQL), para luego lanzar el proceso de backup a cinta y posteriormente enviar a custodia. Todos los backups de Base de datos son Full backup.

Los backup son generados diariamente en el sistema de almacenamiento, pero solo se guarda como histórico para posterior restauración los backups en cinta de los días 5, 10, 15, 20, 25 y último día de cada mes.

En una cinta se almacena los backups generados del día 5, 10 y 15 y en la segunda cinta el día 20, 25 y último día del mes, de las cuales se generan dos cintas de cada una, para lo cual se necesitara al mes un stock de 4 cintas por mes.

Proceso de Borrado de Backup de Base de Datos

Después de realizado el backup en cinta se borran los backup del sistema de almacenamiento y se conservan hacia atrás los últimos 5 días, que luego son borrados secuencialmente.

Pruebas de Restauración de Backup

Como medida de protección durante el año se hará pruebas de las cintas de backup, tanto para las cintas que se envían a custodia externa como las que se resguardan al interior del GT de Soporte Tecnológico.

Las pruebas de restore se realizan cada trimestre y se ha definido los siguientes periodos:

- El 30 de marzo se hace la prueba de restore para las BD de las fechas 31 de Diciembre del Año anterior.
- El 30 de Junio se hace la prueba de restore para las BD de las fechas 30 de Marzo.
- El 30 de Septiembre se hace la prueba de restore para las BD de las fechas del 30 Junio.
- El 30 de Diciembre se hace las pruebas de restore para las BD del30 de Septiembre.

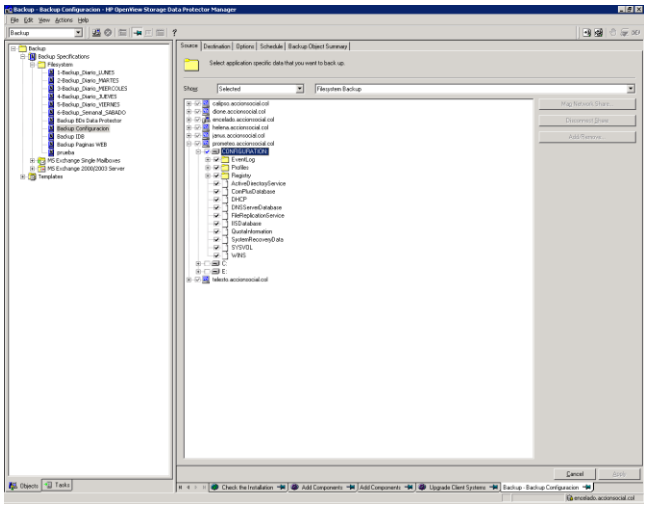
Los resultados serán guardados en la Bitácora de restore. Llamada Planilla de Control de Restore Backups_BD

Backup de la configuración de los Servidores

Para proteger los controladores de dominio y el directorio activo se debe realizar la copia de seguridad del “SystemState” en los dos servidores (TITAN y SKOLL); adicionalmente antes de instalar un nuevo driver (controlador) o una nueva aplicación se debe actualizar el disco de

reparación del sistema, una vez comprobada la correcta funcionalidad del servidor se debe actualizar nuevamente el disco de reparación.

Para esto es necesario utilizar las dos herramientas de backup, tanto la herramienta de Windows (NT_Backup) como la herramienta Data Protector.



Para el backup de la configuración de los servidores se debe realizar a través de Data Protector.

Dado que este Backup cambia poco se toma la decisión de realizar un backup semanal el cual se realizar el domingo en las horas de la noche. Para esto se usa una cinta de 800/1600 GB la cual se reutiliza cada semana. En el backup que se guarda del mes queda incluida una copia de este backup.

Backup de Archivos

Este Backup se realiza a través de la herramienta de Data Protector.

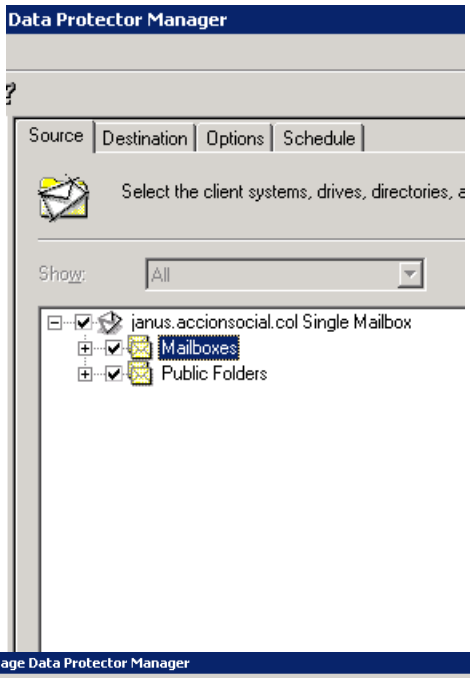
El backup que se realiza de archivos se hace al servidor Calipso y algunas carpetas del servidor Prometeo.

El esquema de backups corresponde a backups diarios de lunes a jueves y un Backup el fin de semana. Para lo cual se utilizan pool de cintas por día de lunes a jueves y un pool de cintas para el fin de semana.

Para lo cual las cintas utilizadas de lunes a jueves se reutilizan cada semana y las del fin de semana se mantienen por un mes y se utilizan al mes siguiente a excepción de la ultimas cintas de fin de semana del mes la cuales se guardan como mensuales y son enviadas a custodia.

Nota: Las cintas utilizadas corresponden al backup que se hace de archivos, Buzones, Bases de Datos de correo y configuración de servidores.

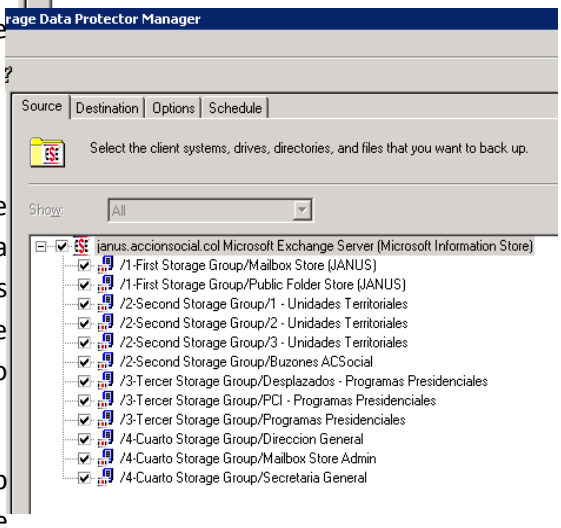
Backup de Buzones



Este Backup se realiza a través de la herramienta de Data Protector.

Este Backup permite realizar backup a cada uno de los buzones de los usuarios.

El esquema de backups corresponde a backups diarios de lunes a jueves y un Backup el fin de semana. Para lo cual se utilizan un set de cintas por día de lunes a jueves y un set de cintas para el fin de semana.



Para lo cual las cintas utilizadas de lunes a viernes se reutilizan cada semana y las cintas del fin de semana se mantienen por un mes y se utilizan al mes siguiente a excepción de la ultimas cintas de fin de semana del mes la cuales se guardan como mensuales y son enviadas a custodia.

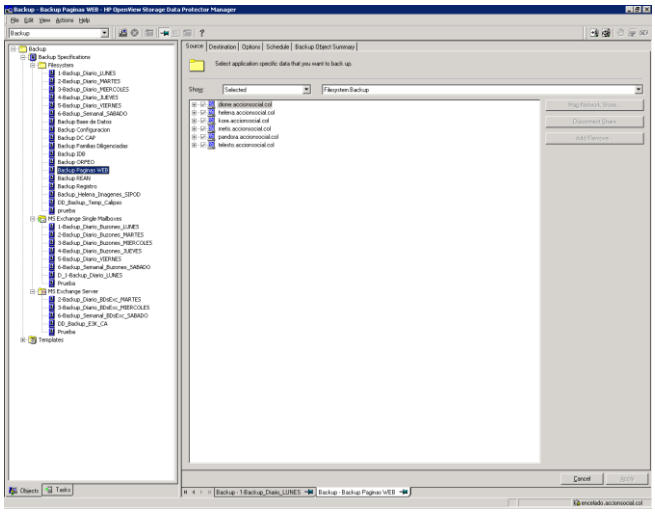
Nota: Las cintas utilizadas corresponden al backup que se hace de archivos, Buzones, Bases de Datos de correo y configuración de servidores.

Backup de Base de Datos Correo Electrónico

Este Backup se realiza con la herramienta Data Protector.

Este backup permite realizar backup a cada una de las bases de datos de Exchange.

Este backup se realiza los fines de semana y se realiza sobre el set de cintas destinado para el fin de semana.



Backup de Aplicaciones WEB

Este Backup se realiza con la herramienta de Data Protector.

Se realiza a los archivos que se encuentran en los servidores que poseen configuradas las aplicaciones Web.

Este backup se realiza una vez por semana el fin de semana en un pool de cintas exclusiva para esto.

Esquema de Backups DPS

Realización de Backups y Tipo

	Backup Tipo Normal				
	Archivos	**Buzones**	**BDs Datos Correo**	**Configuración Servidores**	**Aplicaciones Web**
Lunes	✓	✓			
Martes	✓	✓			
Miércoles	✓	✓			
Jueves	✓	✓			

Sábado	✓	✓	✓		
Domingo				✓	✓

Cintas a Utilizar por Mes

Semana \ días	Lunes	Martes	Miércoles	Jueves	Sábado
1	6	6	6	6	6
2	6	6	6	6	6
3	6	6	6	6	6
4	6	6	6	6	6

Nota: De lunes a jueves se utilizan cada día un set de seis cintas las cuales se reutilizan cada semana, el fin de semana se utiliza un set de seis cintas la cuales se guardan por un mes y al mes siguiente se utiliza reutilizan nuevamente a excepción de las cintas del último fin de semana del mes, la cuales se envían a custodia como el Backup mensual.

Esquema de Custodia de Backups

La Agencia tiene contratado con una empresa el servicio de custodia de medios magnéticos (cintas magnéticas), en un lugar seguro fuera de la institución con condiciones ambientales controladas, sistemas automáticos de extinción de incendios y acceso restringido, como medida preventiva en caso de un desastre o perdida involuntaria de los archivos vitales. Se posee una copia de nuestra información en un lugar seguro y alejado de nuestro centro de cómputo, con disponibilidad 24 horas al día y 365 días al año.

Terminados lo backup a cinta se envía un correo electrónico a la empresa contratada para que el día siguiente pasen y recojan las cintas. Para asegurar el respaldo de cintas fuera de la entidad. Esto va de la mano con el plan de contingencia que se posee.

Luego de realizar los backups y definir las cintas que se van a enviar a custodia, el funcionario responsable de los Backups llena un formato en Excel (Planilla Control de backups) donde se relaciona el catálogo de la cinta con los datos que esta tiene.

Proceso de Entrega de Medios Para la Custodia

El proceso de entrega de los medios se hace quincenalmente, las cintas con información de las bases de datos son guardadas en la entidad en una caja fuerte mientras son entregadas al contratista, la entrega se hace a personal debidamente identificado.

Para la entrega de las cintas se llena un formato donde se indica la fecha de entrega, la cantidad de cintas con su respectivo rotulo; Los formatos de relación de catálogos con datos y formato de entrega son almacenados en una carpeta que se encuentra archivada en el área del GT se Soporte Tecnologico.

Tipo de Transporte Contratado

El transporte se brinda desde las instalaciones del DPS hasta la empresa contratada y viceversa según las solicitudes del área de sistemas en las siguientes modalidades

Normal: de Lunes a Viernes de 7:45:a.m. a 5:15 p.m., Se envía correo a la empresa encargada para que recojan o entreguen medios, se conviene el día y hora con el contratista durante el término del contrato programada con 24 horas de anticipación en horario hábil

Extraordinario: Solicitud de servicio programado con 4 horas de anticipación en horario hábil (de 7:45:a.m. a 5:15 p.m. de lunes a viernes).

Emergencia: Solicitud de servicio programado con 4 horas de anticipación en horario no hábil.

Área de Almacenamiento

Los medios magnéticos son almacenados en un área especial de seguridad, climatizada a temperatura y humedad constantes, para su normal conservación. El área de almacenamiento, está dotado de sistemas de control de humedad que mantiene un rango de 15% a 60% y una temperatura controlada automáticamente que oscila entre 15 y 20 grados centígrados. Adicionalmente posee puerta de seguridad, censores fotoeléctricos de movimiento, inundación, intrusión e incendio y circuito cerrado de televisión. El acceso a dicha área es restringido y limitado.

Transporte y Consulta de Información

La empresa contratada presta los servicios de traslado de los archivos magnéticos entre las instalaciones de ambas partes, o a los lugares que se indique, bajo ciertas normas de seguridad o acuerdos previamente establecidos en los que se especifique por escrito y previa autorización

dichas entregas. El servicio de transporte se realiza puerta a puerta y las 24 horas del día en vehículos suministrados por la firma proveedora del servicio, los cuales deben poseen sistemas de comunicación continua, tripulados por dos funcionarios, con las medidas de seguridad necesarias para este tipo de servicio.

Las entregas o recibos de información se hacen por personal autorizado previamente por el DPSy la firma prestadora del servicio, los envíos o remisiones se hace por medio de una remesa en la que se relaciona el material entregado uno a uno, contenido y cantidad, de la cual queda copia para cada una de las partes.

Aspectos de Seguridad

Dentro de los sistemas de seguridad física implementados se tiene:

Cámaras de Televisión

Contactos Magnéticos

Sensores Infrarrojos

Centro de Información "CDS"

Sistemas de Detección de Incendios

Sistema Automático de Extinción de Incendios

Sistema Manuales de Extinción de Incendios

Sensores de Inundación

Control de Roedores

Control de Insectos

Prevención, detección y control de hongos

Equipo de Control de Temperatura y Humedad

Prevención, detección y control de Energía.

Planta Eléctrica de Emergencia

Sistemas de UPS

Anexo E. Guía de desarrollo de software

TABLA DE CONTENIDO

INTRODUCCIÓN

Los sistemas de información de la Entidad soportan la operatividad de los procesos y alojan la información como insumo valioso; por tanto definir normatividad en el tema, genera un esfuerzo y motivación justificada. La Entidad cuenta con Sistemas de Información Misionales y de Soporte, de los cuales algunos han sido desarrollados internamente, otros desarrollados por terceros y otros adquiridos a Empresas de Software, por lo cual es necesario e importante estandarizar los procesos de ingeniería de software.

Este documento tiene como propósito, el establecimiento de un marco guía para el desarrollo interno o externo de sistemas de información para el Departamento para la Prosperidad Social.Es un compendio de toda la información necesaria para realizar el análisis, desarrollo e implementación de los sistemas de información, siguiendo un hilo conductor y bajo referencias recientes en la materia.

Se pretende también unificar conceptos relacionados con las prácticas para el desarrollo de software que sean aplicables a las áreas misionales, estratégicas, de apoyo y a otras que sean necesarias en la Entidad, es por ello, que complementariamente se pretende identificar tipos de actores, participantes, roles, documentación, responsabilidades y modelos de operación para labores o proyectos de desarrollo de software y específicamente a través de su ciclo de vida, ya que es importante organizar y agrupar las mínimas actividades a desarrollar en cada una de las fases de los procesos de desarrollo de software relacionadas a los recursos que intervendrían.

ADVERTENCIA

El presente documento contiene información confidencial para uso exclusivo del Departamento Administrativo para la Prosperidad Social DPS.

Quién tenga acceso a este documento debe tomar todas las medidas necesarias para evitar que la información contenida en este documento sea revelada a terceros no autorizados, o que sea utilizada para propósitos diferentes a las actividades de Desarrollo de Software para el DPS.

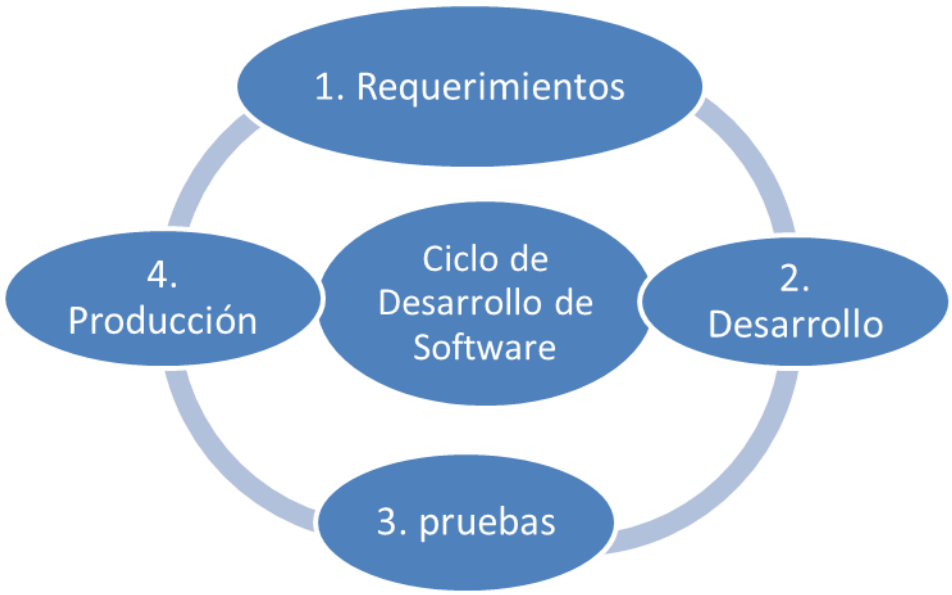
El incumplimiento de esta restricción de confidencialidad constituye falta grave que puede conllevar a sanciones administrativas o legales.

ALCANCE

Los lineamientos establecidos en este documento rigen para todos los funcionarios y colaboradores del Departamento Administrativo para la Prosperidad Social - DPS que intervengan de alguna forma en actividades de desarrollo de software y deberán ser acatadas por todas aquellas personas que en el ejercicio de sus labores interactúen con los servicios y recursos de la Entidad tanto en forma directa como indirecta (Proveedores, Consultores y Asesores, usuarios externos u otros terceros).

1. CICLO DE VIDA DE DESARROLLO DE SOFTWARE

Las actividades del ciclo de vida en el desarrollo de softwarepara el DPS se han asociado en las siguientes fases: especificación de requerimientos, desarrollo, pruebas, puesta en producción y mantenimiento.



1.1 Especificación de Requerimientos

En estas fases se especifican las características funcionales y no funcionales que deberán cumplirse para los siguientes casos: Desarrollo de un componente de software o sistema de información nuevo, modificación a componentes de software o sistemas de información existentes, mantenimiento a componentes de software o sistemas de información ya finalizados.

Estos requerimientos deben estar soportados mediante una solicitud formal o ticket, con el cual se permita realizar la trazabilidad de los cambios solicitados.

Se contemplan tres tipos de solicitudes:

- Creación de nueva funcionalidad o módulo adicional.
- Modificación de un módulo o funcionalidad.
- Corrección de errores de una funcionalidad.

Las solicitudes de creación y/o modificación de una funcionalidad deben ser acordadas entre el área funcional (área solicitante) y el equipo de desarrollo y deberán quedar consignados en un documento DERS (Documento de Especificación de Requerimientos de Software), el cual contiene los elementos básicos o marco de trabajo básico que se debe cumplir, diligenciar e incluir para cada solicitud, de forma más detallada.

Esta solicitud, debe ser realizada a través del líder funcional que es el colaborador de la Entidad designado como enlace entre el área funcional y el equipo de Desarrollo.

1.2 Desarrollo de Software

Se realizan las tareas de programación o codificación de software, las cuales consisten en llevar a código fuente en el lenguaje de programación definido las funcionalidades conforme a lo establecido en la especificación de requerimientos.

Para cumplir las actividades de Desarrollo de Software deben tener en cuenta lo siguiente:

1.2.1Ambiente de Desarrollo

Este ambiente comprende el entorno de desarrollo de una aplicación y es donde se construyen los artefactos que constituyen un sistema. A este ambiente, pueden acceder solo los integrantes del equipo de desarrollo y deben tener los privilegios para crear, modificar y eliminar los artefactos que componen o compondrán el sistema; deben estar restringidos los accesos a los usuarios finales o cualquier otro usuario diferente al equipo de desarrollo.

Estas prácticas, aplican tanto para los repositorios de datos como para servidores de aplicación. Se debe establecer un Ambiente de Desarrollo para cada aplicación. Este ambiente debe ser independiente y aislado del ambiente de pruebas y del ambiente de producción.

1.2.2 Políticas de Gestión de Configuración.

Para realizar la administración del ciclo de vida de las aplicaciones se define como plataforma Microsoft TeamFoundation Server (TFS). Cada aplicación nueva y sus artefactos (código, compilados, ejecutables, documentación, scripts de base de datos) deben ser administrados por el TFS. Esta plataforma es administrada por el grupo de infraestructura y soporte.

Se debe realizar la creación de un nuevo TeamProyect por cada nueva solución. Las soluciones solo deben ser creadas para enmarcar un conjunto de proyectos que hacen parte de un mismo sistema de información, no se deben crear nuevos TeamProyect para una aplicación si el sistema al cual pertenece ya tiene creado un TeamProyect.

La plantilla que debe ser utilizada para cada nuevo TeamProyect es la plantilla Scrum, preferiblemente en la última versión, aunque se pueden utilizar también las plantillas CMMI y MSF.

Cuando se cree un nuevo TeamProyect o cuando se registren cambios en el equipo de desarrollo, el líder de desarrollo debe enviar al grupo de Infraestructura y soporte, el listado de usuarios y privilegios que harán parte de este; esto para garantizar la seguridad sobre los artefactos que reposan en el servidor, la comunicación la puede realizar mediante canalización a través de la mesa de ayuda, correo electrónico o por la forma establecida por el coordinador del Grupo de Trabajo de Infraestructura y Soporte de Tecnologías de Información.

Cada aplicativo deberá contar con una estructura de directorios que permita diferenciar los tipos de artefactos que almacena, de la siguiente forma:

- Base de Datos: procedimientos almacenados para realizar control de código fuente, diagramas E-R, scripts, documentación de base de datos, backup de bases, bases de pruebas etc.

- Código: código fuente, artefactos y ensamblados de la aplicación (ver Lineamientos de desarrollo para detallar esta carpeta).

- Documentos: documentación del proyecto, casos de uso, DERS, documentos de análisis, presentaciones del sistema y en general toda la documentación sobre el proyecto.

Nota: Esta estructura debe quedar almacenada en el servidor Team Server y controlada

1.2.3 Plataforma de Desarrollo

Los sistemas deberán estar desarrollados sobre plataformas WEB o desconectadas, utilizando:

TEMA	DESCRIPCION
Sistemas Operativos de Servidores	Plataforma Microsoft 2008 Server y/o versión más reciente.
Base de datos Relacional	Oracle (Actualmente 11G o versión más reciente) SQL Server (actualmente versión 2008R2 o versión más reciente)
Servidor WEB	Versión más reciente plataforma Microsoft Internet Information Server IIS (Actualmente IIS 7.0)
Entorno de desarrollo	Versiónmás reciente de la Plataforma Microsoft Visual Studio.NET (Actualmente framework 4 y entorno Visual Studio 2010)
Lenguaje de programación	C#
Browser	Internet Explorer 8.0 o superior

1.2.4Lineamientos para el Manejo de la Base de Datos

- El manejo de la información debe hacerse a través de procedimientos almacenados.
- Se debe utilizar índices sobre los campos de búsqueda para mejorar el tiempo de respuesta de las consultas.
- Uso de un Modelo Entidad – Relación
- Se debe realizar normalización de las bases de datos estas deben alcanzar como mínimo la cuarta forma normal 4N, se recomienda hacer la normalización hasta la quinta forma normal con el fin de quitar la responsabilidad a la aplicación en la consistencia de los datos.
- Se debe documentar todos los objetos de la base de datos. En el modelo relacional cada tabla debe guardar una descripción de su uso, así como cada campo en la tabla debe ser descrito indicando para que se utiliza el campo.Ejemplo:

Table CABILDO

tabla que contiene la definicion de cabildos indigenas

Columns

Name	Type	Optional	Default	Comments
CODCABILDO	NUMBER			codigo unico de cabildo
CODMUNICIPIO	VARCHAR2(5)			codigo del munipio del cabildo
CABILDO	VARCHAR2(50)	Y		nombre del cabildo

Primary Key

Name	Columns
CABILDO_PK	CODCABILDO,CODMUNICIPIO

Foreign Keys

Name	Columns	Referencing Table	Columns
CABILDO_MUNICIPIO_FK	CODMUNICIPIO	MUNICIPIO	CODMUNICIPIO

Indexes

Name	Columns	Type
CABILDO_PK	CODCABILDO,CODMUNICIPIO	Unique

- Para los procedimientos almacenados se debe agregar un comentario al inicio donde se especifique su funcionalidad e indicar parámetros de entrada y salida así como la fecha del último cambio y el responsable del cambio. Ejemplo:

```
CREATE OR REPLACE PROCEDURE usp_nombre_del_procedimiento
(  pNombreParametro IN NUMBER,
  cur_OUT OUT accionsocial.cursor_select)
-------------------------------------------
-- Fecha de Creacion (dd/MM/yyyy): 25/05/2007
-- Creador: nombre del creador
-- Descripcion: describir que hace el procedimiento
-- Cambios      agregar estas lineas y colocar el nombre de quien realiza el cambio
-- Fecha:       fecha del cambio
-- Descripcion: descripcion del cambio
-------------------------------------------
IS
BEGIN
  ...--lineas del procedimiento
```

- Para la utilización de parámetros se debe nombrar cada parámetro iniciando con la letra p (ejemplo: PNombre), esto con el objeto de evitar errores en la ejecución del script ya que puede presentarse algún nombre de campo de alguna tabla con el mismo nombre del parámetro utilizado, apareciendo errores en la consulta difíciles de detectar.

- Se debe establecer el usuario en la base de datos que consumirá la aplicación con los privilegios para cada uno de los objetos que consulte, inserte o actualice respectivamente, en ningún caso se debe tomar el usuario propietario del esquema o el SA como el usuario de la aplicación. Se debe indicar al Administrador de Base de Datos (DBA), formalmente los permisos que debe tener el usuario que ejecutará la aplicación para cada tabla (DELETE, UPDATE, INSERT)

- Se debe seguir con la tabulación para la creación del script con el fin de hacer legible el código.

1.2.5Lineamientos para el Manejo del Desarrollo

- La aplicación o sistema debe ser construido siguiendo un desarrollo en N-Capas, separando claramente como mínimo la capa de presentación, la lógica de negocio y el acceso a datos. El objetivo del diseño es que las capas no queden acopladas fuertemente para que la solución sea flexible a los cambios. Cada capa debe tener claramente delimitada su responsabilidad, de igual forma cada capa únicamente se comunica con su capa inferior o su capa superior, no debe existir comunicación entre capas que no sean inmediatas ya sea por su nivel inferior o superior.

- Se debe usar el Modelo Orientado a Objetos.

- Los métodos y procedimientos desarrollados deben tener documentación en la que se especifique la funcionalidad, las entradas y las salidas, para esto utilizar el estándar de

comentarios proporcionado por Visual Studio, documentando la responsabilidad de cada clase, el uso de cada parámetro, método y evento. Ejemplo:

```
namespace EspacioNombres
{
    /// <summary>
    /// Clase para ...descripcion de la responsabilidad
    /// </summary>
    class NombredeClase
    {
        /// <summary>
        /// descripcion de la función
        /// </summary>
        /// <param name="parametro1">codigo del parametro de busqueda...descripcion del parametro de
        /// entrada indicando que es</param>
        /// <returns>descripcion de que sale del método</returns>
        public string NombreDelMetodo(string parametro1)
        {
            string salida = "";
            try
            {
                //comentarios adicionales para entender la funcionalidad si son necesarios
            }
            catch (Exception ex)
            {
                throw ex;
            }
            return salida;
        }
```

- Uso de caché para disminuir al máximo la llamadas al servidor si se construyen aplicaciones web.
- Se debe utilizar Windows CommunicationFoundation (WCF) para la creación de servicios.
- Se debe validar las entradas desde la capa de presentación.
- Uso de ayudas para agilizar la digitación en las interfaces de captura.
- Uso de tooltips.
- Manejo ágil de listas y combos para la selección de opciones con una cantidad no mayor a 200 ítems o utilización de filtrado inicial para resultados de más de 200 ítems.
- En caso de hacerse necesario el uso de lenguajes Script jscript, deben hacerse llamados a funciones contenidas en archivos Script.

1.2.6 Guíapara la Estructuración de Proyectos y Soluciones (Plataforma Visual Studio)

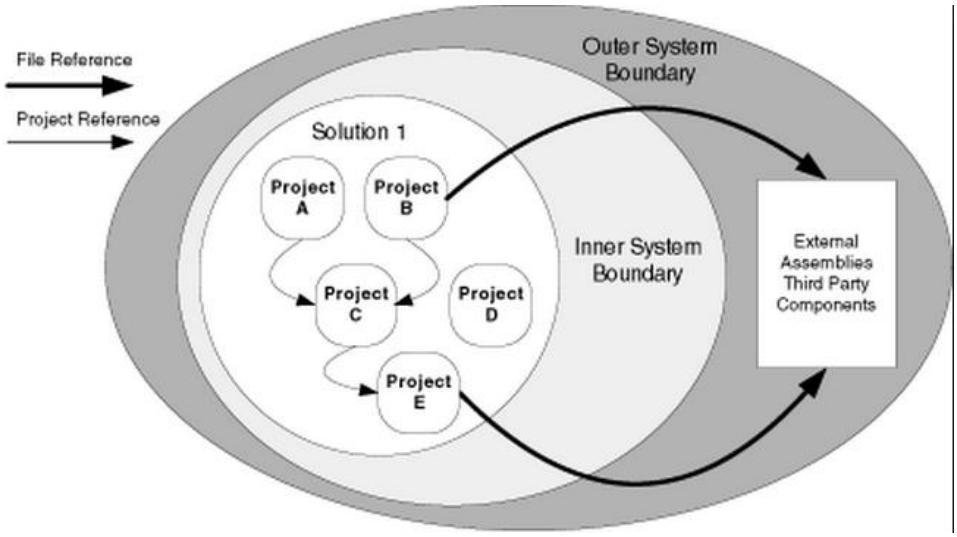
Para el manejo de un nuevo sistema se pueden abordar tres tipos de alternativas para crear la estructura del proyecto en Visual Studio:

1.2.6.1 Crear una Única Solución: Crear una solución de Visual Studio para agregar varios proyectos, esta debería ser la primera opción a considerar siempre y cuando la cantidad de proyectos no sea demasiado grande para ser manejada por Visual Studio obteniendo un buen tiempo de respuesta. Las ventajas que presenta es tener todas las referencias en una misma solución eliminando las referencias a archivos así como facilitando la actualización de los compilados de cada proyecto con cada construcción, ya que todas las referencias entre ensamblados del proyecto se deberían llevar como referencias hacia proyecto.

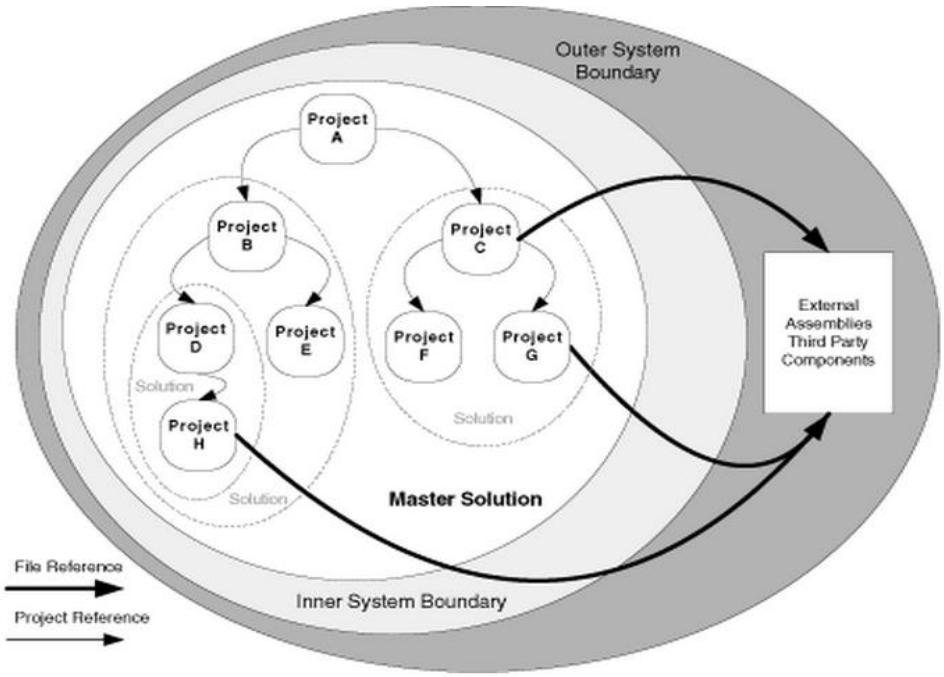
1.2.6.2 Particiones de una Solución: Esta opción debe ser considerada si se tiene una gran cantidad de proyectos y que hacen que su manejo en visual Studio presente grandes tiempos en la carga o en la compilación o cuando lógicamente la solución puede tener múltiples vistas diferentes y desarrolladas por equipos con responsabilidades diferentes. La partición de la solución se hace a nivel lógico, cuando las responsabilidades de un grupo de proyecto son claramente diferenciadas. Dentro de este tipo de soluciones se pueden encontrar referencias a archivos de ensamblados de otras soluciones con lo cual se debe tener especial cuidado para el manejo de versiones tomando las versiones más recientes de los archivos de ensamblados. Pueden crearse soluciones independientes y utilizar una única solución que agrupe el conjunto de soluciones individuales.

1.2.6.3 Múltiples Soluciones: Utilizar solo cuando se tengan sistemas muy grandes que requieran ser partidos en subsistemas, ubicando cada subsistema dentro de una solución con múltiples proyectos.

Se recomienda la utilización de una única solución haciendo fácil el manejo de referencias así como la instalación de la solución en un nuevo equipo o el entendimiento del proyecto para un nuevo miembro del equipo de desarrollo, ya que las referencias se mantienen actualizadas con cada rebutid de la solución. Igualmente se pueden seguir utilizando referencias a archivos o compilados externos a la solución, estos deben visualizarse como referencias a componentes o archivos de terceros y por lo tanto deben quedar por fuera de la solución. Cuando existan referencias a ensamblados generados por otros proyectos pero que estén dentro de la misma solución deben crearse referencias a proyecto (Project Reference) esto por ejemplo para el caso de aplicaciones de N-Capas cada capa genera un Assembly y la referencia de la capa superior a esta debe hacerse por proyecto a la capa inferior.



- Para particiones de una solución opte por crear una solución maestra que contenga varias soluciones para permitir a los desarrolladores trabajar con alguna parte de los proyectos sin tener que cargar todas las soluciones:



- Para cada solución se recomienda la utilización de directorios para cada tipo de proyecto. Un ejemplo de esto es que se pueden tener varios proyectos en una solución con

tecnologías diferentes por ejemplo proyectos web ASP.NET, proyectos de WinFormsasí como WPF, WCF, Web Services etc.

De esta manera se pueden tener varios proyectos y varios folders para cada proyecto enmarcado en la tecnología que utiliza. Ejemplo:

1.2.7Lineamientos para el Manejo de la Seguridad de las Aplicaciones

El manejo de la seguridad a nivel de la aplicación deberá contemplar los siguientes aspectos:

- Permisos sobre procedimientos almacenados únicamente, En cuanto a la base de Datos (evitan la inyección).

- Mantener la secuencia lógica entre las pantallas. (no entrar directamente a una página que deba ser accesada desde otra. Acceso únicamente a través de la secuencia de navegación).

- Para el acceso a las interfaces se debe validar la autorización del usuario durante la sesión.

- Cuando los aplicativos son utilizadas solo por usuarios internos, se debe implementar haciendo uso del directorio activo del sistema operativo.

- Se debe Implementar seguridad de acceso sobre las paginas (Utilizar tiempos de inoperancia de las paginas, evitando que la sesión de la página quede abierta).

- Para gestionar el control de acceso de usuarios al aplicativo o funcionalidad, se debe tener en cuenta la implementación de los siguientes esquemas de seguridad:

    - Guardar número de intentos fallidos de acceso a la aplicación por parte de usuarios potenciales.
    - Almacenar la dirección IP de la ruta de acceso que intento el ingreso.
    - Establecer estándar para los usuarios y contraseñas, clasificando niveles y considerando tipos de caracteres.
    - Bloqueos a cuentas por intentos fallidos.
    - Obligar a cambios periódicos de contraseñas.
    - Revocar los permisos de acceso tras no haber ingreso al sistema en un tiempo determinado, con el objetivo de eliminar usuarios no deseados o desvinculados.
    - Permitir bloqueo a usuarios que ya no pertenecen a la organización o inactivos.

- Definición de perfiles de usuario (Asignación de privilegios sobre las operaciones a realizar sobre la aplicación.)

- Se debe utilizar técnicas de encriptación.

- Utilizar la seguridad basada en roles para asegurar que funcionalidades o recursos propios de un tipo de usuarios no sean utilizados por otro, así sean usuarios validos de la aplicación. La utilización de roles simplifica la administración de usuarios.

- Evitar al máximo el uso de componentes ***com***o componentes no administrados, ya que esto debilita el modelo de seguridad que puede dar ***.Net***.

- Las aplicaciones se deben ejecutar con los mínimos privilegios posibles sobre el sistema operativo.

- Se debe considerar prepara el desarrollo para que la autorización de permisos solo sea realizada modularmente y mediante un proceso de canalización (No se permitirán herencia de permisos)

- De requerirse hacer llamados a otras ensamblados (Ejemplo: ***.exe, dll***) se debe utilizar permisos por demanda para evitar que un intruso llame ensambladores con un nivel de permisos menores (este tipo de seguridad valida que todos los que realizan la llamada tengan los por lo menos los mismos permisos).

- Para el acceso a funciones sensible del aplicativo utilizar la definición de permisos declarativamente es decir por código fijar la seguridad ya sea a una clase o a un método.

- La instalación de la aplicación debe hacerse por medio de un programa de instalación en donde se encuentre embebido las políticas de seguridad.

1.2.8Lineamientos para el Manejo de Errores, Advertencias y Excepciones

- La interface se debe validar a nivel de campo (controlar longitud, tipo, formato, dependencia, etc), a nivel de página (mensaje en caso de fallo de la transacción, generando un registro de estos, verificar la obligatoriedad de campos y manejar un timeOut razonable para la vigencia de la página), a nivel de transacción (validar integridad referencial y manejo de transaccionalidad).

- La visualización del error debe ser lo menos dicientes en aspectos técnicos y descripción del sistemas, se debe visualizar un mensaje claro para usuario final y en la bitácora de errores o en un log hacer la descripción técnica del error.

- Se recomienda la utilización de EnterpriseLibrary en su última versión disponible para el manejo de excepciones, capturando el error dándole tratamiento y dejando un log o base de datos con los errores reportados por la aplicación con el fin de dar seguimiento y solución a estos.

- La presentación de los mensajes de errores, advertencias y excepciones que deben ser presentados a los usuarios de los sistemas de información por la misma máquina, deben ser

generados de forma clara para el usuario y deben presentar una o varias sugerencias posibles de solución.

- Para el manejo de excepciones se debe siempre usar bloques try catch y finally
- Validar las entradas del usuario utilizando expresiones regulares.
- Sanear las entradas del usuario es decir no dejar pasar campos nulos ni con espacios ni caracteres inválidos, delegar esta responsabilidad a la capa de presentación.
- Indicar al usuario de forma clara y señalizada los campos obligatorios para diligenciamiento en formularios web.

1.2.9Lineamientos para el Manejo de Registros de Transacciones en Base de Datos.

Es necesario establecer registros para las transacciones realizadas en la aplicación, en los movimientos que insertan, eliminan y actualizan información, por medio de las cuales se registre la actividad de los usuarios en el sistema. Dichos registros deben contener como mínimo la siguiente información:

- Usuario que realiza la transacción: Implementar un mecanismo que permita identificar con claridad nombres y apellidos del usuario (funcionario).
- Fecha y hora de realización.
- Instrucción ejecutada.
- Tabla que se modifica.
- Registro que indique como estaba la información antes de ser modificada o eliminada que facilite reconstruir los datos antes de producirse el cambio.

El almacenamiento de transacciones se debe habilitar para las entidades de la base de datos que comprendan los módulos principales y más importantes del sistema de información

1.2.10Lineamientos Para el Manejo de datos Históricos.

Un Almacén de Datos contiene una gran cantidad de información (datos históricos) especialmente diseñada para realizar análisis estratégicos sobre la información que contienen. Esta información suele ser muy útil para la toma de decisiones de la entidad.
Se deben diseñar e implementar medios y procesos de generación y almacenamiento de información histórica a partir del manejo de campos de estado y fechas para que se controlen los cambios generados dentro del sistema por los procesos de ingreso, actualización y modificaciones a registros; además el sistema deberá estar en capacidad de generar los diferentes documentos que se afectan por dichas operaciones generando cada uno de los documentos del registro a una fecha de corte dada.

Se debe seleccionar la mejor estrategia de diseño del almacén de históricos en virtud de la cantidad de registros relacionados, el tipo de base datos, el tipo de soporte para copias de seguridad y especialmente del tipo de negocio para el cual es diseñada la base de datos principal.

1.2.11Lineamientos para el Manejo de Reportes y Consultas

- La plataforma para el manejo de reportes de información transaccional es ReportingServices en su versión más reciente.
- Los reportes deben ser ejecutados por el servidor no en modo local.
- Los reportes deben estar almacenados en el servidor de reportes.
- Los reportes que se realicen deberán permitir previo a su impresión o envió a algún medio de almacenamiento la consulta por pantalla.
- Se debe establecer niveles de acceso de uso de los reportes por perfil
- Los reportes a desarrollar deberán ser de tres tipos: estáticos, parametrizables, dinámicos. De acuerdo con el proceso y cliente
- Los reportes estáticos serán los que de forma estandarizada y periódica se requieren con destino a usuarios finales con quienes se tiene definido un protocolo y formato de salida.
- El uso y entrega de reportes periódicos por medio del envío vía email debe realizarse utilizando la suscripción de reportes de ReportingServices.
- Los reportes parametrizables serán aquellos en los que los formatos predefinidos se producen de acuerdo con la selección de variables de entrada, de escogencia del usuario.
- Los reportes dinámicos serán los que presenten al usuario las variables y procesos que aplica el sistema para que sea el usuario quien componga en forma libre y autónoma el reporte deseado respetando en todo caso las restricciones que el modelo defina.
- Se deberá tener la opción de salidas de información tanto a impresora local y/o remota, archivos planos, hojas electrónicas y pdf.

1.2.12Lineamientos para la Administración del Sistema

La herramienta debe contar con la facilidades de creación de usuarios, roles, perfiles y grupos de trabajo generando un esquema de funcionamiento seguro, donde los accesos y transacciones puedan ser eficientemente controladas. La administración del sistema deberá contener:

- Definición de grupos, perfiles de usuarios y niveles de acceso

- Administrar la seguridad de acceso a nivel de grupos y usuarios.
- Administrar las tablas de referencia.
- Asignar permisos que permitan ejecutar los módulos con los parámetros de configuración seleccionables.
- Administración de la auditoria

Nota: En los casos que se requiera por las consideraciones de seguridad de la aplicación se podrá generar aplicaciones cliente servidor para la administración del sistema.

1.2.13Lineamientos para el Manejo de Ayudas del Sistema y Utilidades

La ayuda en línea permite al usuario resolver dudas, conocer la operación básica de los módulos del sistema, determinar errores que se cometen frecuentemente al operarlos y la manera de corregirlos. La navegación a través de la ayuda, la búsqueda de términos, párrafos, páginas y otras referencias agilizan la navegación a través del documento electrónico y la impresión de sus contenidos, como mínimo se requiere:

Permitir la consulta de:

- Documentos de explicación del uso de la herramienta.
- Documentos normativos.
- Documentos de conceptos jurídicos.
- Documentos de respuesta a preguntas frecuentes.
- Glosario de términos referentes al sistema como herramienta técnica y otros referentes al sistema como soporte conceptual.
- Vínculos a sitios web de interés.
- Facilidad para mensajes emergentes desde la administración del sistema a todos los usuarios conectados a la aplicación.

1.2.14 Documentación Aplicable a Las Aplicaciones

Toda aplicación que entre a un ambiente de producción debe contar con los siguientes documentos y manuales con el fin de hacer más fácil la utilización de la aplicación así como para reducir los tiempos de mantenimiento y la adopción rápida por un nuevo equipo de desarrollo así como nuevos usuarios finales:

- **Manual de Usuario**: Este documento es dirigido al usuario final de la aplicación, de manera que sirva de guía para su utilización y es donde se describen las funcionalidades y

bondades del sistema así como la mejor manera de utilizarlo. Debe incluir como mínimo la siguiente información:

- Tabla de Contenido, versión del documento e introducción
- Descripción general del sistema y su contexto.
- Descripción de la interfaz de usuario y modelo de navegación.
- Descripción módulos del sistema.
- Descripción mensajes de error.
- Descripción de salidas.

- **Manual Técnico.** Este documento contiene la información concerniente a los aspectos técnicos de la aplicación debe estar compuesto como mínimo por la siguiente estructura:

  - Introducción y versión del documento.
  - Modelo general del sistema.
  - Documentación de la arquitectura del sistema.
  - Plataforma tecnológica.
  - Documentación de base de datos.
  - Diagrama E-R o Modelo Relacional.
  - Diccionario de datos.
  - Descripción de código fuente:
    - Descripción de la estructura de la solución.
    - Ubicación de las fuentes para cada proyecto.
  - Para proyectos de inteligencia de negocios descripción de cada artefacto su funcionalidad y uso así como su ubicación en desarrollo y producción para AnalisysServices, IntegrationServices y ReportingServices.
  - Inventario de reportes.

- **Manual de Instalación.** Este documento describe las condiciones para realizar la instalación, así como la plataforma requerida y los pasos detallados de configuración para el despliegue en producción de la aplicación, debe contener como mínimo:

  - Requerimientos.
  - Procedimiento de instalación
  - configuración del sistema (parámetros y ajustes a tener en cuenta).

1.2.15 Imagen Institucional

El diseño gráfico se debe realizar de acuerdo con la imagen institucional y parámetros definidos en **el Protocolo de Comunicaciones de la entidad**. Para aplicaciones web se deben utilizar hojas de estilo (CSS), de forma que el aspecto de los elementos de la interfaz puedan ser alterados fácilmente cambiando únicamente la hoja de estilos.

1.3Actividades de Calidad y Pruebas de Software.

En este grupo de actividades, se realiza la revisión, verificación y validación de los desarrollos realizados con el fin de que se cumpla la funcionalidad o funcionalidades requeridas y planeadas en las Actividades de Ingeniería de Requerimientos.

Para lo anterior es responsabilidad del Área Funcional o Área u órgano Solicitante, realizar las pruebas necesarias para revisar el adecuado funcionamiento de las funcionalidades, se deben ejecutar pruebas de validación de datos, pruebas al sistema verificando el flujo de información, y la funcionalidad.

Así mismo, debe realizar pruebas de integración, las cuales deben asegurar el correcto funcionamiento del sistema completo al operar e interoperar en conjunto.

Se deben realizar pruebas en diferentes contextos, así:

- **Pruebas de Desempeño**: Revisar el tiempo de ejecución de las funcionalidades y el consumo de recursos de máquina, tanto locales como de servidor.

- **Pruebas de Resistencia**: Consiste en forzar la aplicación para revisar hasta donde resiste, causando volúmenes de datos altos, concurrencias masivas, etc.

- **Pruebas de Seguridad**: Consiste en evaluar si la aplicación y sus mecanismos de protección funcionan adecuadamente.

- **Pruebas de Recuperación**: Allí se busca que la aplicación falle y revisar en cuánto tiempo y en qué forma se puede restablecer.

La retroalimentación de las pruebas se realizará mediante una Acta, que debe remitirse a los encargados del desarrollo, supervisores, coordinador y/o lideres encargados de los proceso de desarrollo de software en la entidad, que deberá tener por lo menos las siguientes variables: Número de la Prueba, Nombre del Caso de Prueba, fecha de la prueba, categoría de la prueba, incidencia o resultado, posible corrección y/o ajuste, responsable del caso de prueba. El medio de envío de este documento será por la Mesa de Ayuda por correo electrónico en su defecto.

1.3.1 Ambiente de Pruebas

El ambiente de pruebas es utilizado para desplegar el sistema una vez se tenga desarrollada una nueva funcionalidad y se encuentre en condiciones de ser probada por el usuario final, esto como paso previo a su puesta en producción.

Se establece como condición para el despliegue en este ambiente, la validación por parte del equipo de desarrollo de la inexistencia de errores de codificación, así como el manejo de excepciones no previstas que se puedan presentar.

El entorno de pruebas debe ser lo más cercano en el aspecto técnico al ambiente de producción, de manera que se pueda desplegar en producción la misma configuración y obtener en las pruebas los datos de rendimiento esperados en producción así como detectar en este entorno los posibles problemas.

Cada desarrollo puede contar con uno o más ambientes de pruebas, de tal forma que se puedan tener más de una versión del sistema para pruebas. El ambiente se compone tanto del repositorio de datos, datos de pruebas así como los componentes de software.

Este ambiente debe estar aislado del ambiente de desarrollo y del ambiente de producción.

Este ambiente debe ser controlado por el Grupo de Infraestructura y Soporte de TI y el despliegue de una aplicación o de alguna modificación debe ser solicitado formalmente por el equipo de desarrollo mediante un correo electrónico o por la Mesa de Ayuda sobre el ticket ya creado de la solicitud inicial de desarrollo.

1.4 Fase de Producción

La fase de producción es aquella durante la cual el sistema cumple las funciones para las que fue desarrollado, es decir, es finalmente utilizado por el (o los) usuario final.

1.4.1 Ambiente de Producción

En este entorno se despliegan los componentes de software ejecutables que pasan a ser utilizados por los usuarios finales. Solo se pasan a este ambiente los desarrollos que hayan superado la fase de pruebas, para esto el área usuaria o su representante deberá formalizar el paso a producción con una aprobación del desarrollo, la cual es formalizada mediante una acta, a través dela mesa de ayuda o por correo electrónico en su defecto.

Para realizar el despliegue en producción de los componentes compilados o ejecutables se tomarán las versiones probadas y aceptadas del ambiente de pruebas, en ningún caso se tomarán directamente desde el ambiente de desarrollo.

El Grupo de Trabajo de Infraestructura y Soporte de TI, será el responsable de la administración de la aplicación o el sistema en este ambiente. Los datos que se encuentran en el ambiente de producción así como su estructura no deberán ser modificados, por lo tanto la custodia de estos, así como el aseguramiento de su integridad será responsabilidad de este grupo.

Los datos solo podrán ser modificados en su contenido por medio de la aplicación que hace parte del sistema correspondiente. Si por alguna razón existe la necesidad de modificar o agregar datos y la aplicación no soporta la funcionalidad requerida para esta labor se podrán realizar estas modificaciones solo mediante comunicación escrita por el Líder Funcional y aprobada por el coordinador del proyecto de software del DPS, que podrá ser de la Oficina de Tecnología de Información o del Grupo de Trabajo de Infraestructura y Soporte de Tecnología de información, la aprobación deberá quedar certificada mediante Acta o en su defecto correo electrónico en el cual

se especifique el detalle del motivo cambio de datos, base de datos, estado actual, tipo de la modificación, sistema de información afectado, fecha, cantidad de registros afectados.

1.5 Mantenimiento

El mantenimiento del software, es el proceso de control, mejora y optimización del software ya desarrollado e instalado, que también incluye depuración de errores y defectos que puedan haberse filtrado de la fase de pruebas de control. Esta fase es la última que se aplica al ciclo de vida del desarrollo de software.

Si surge un ajuste o una modificación en un sistema de información, es responsabilidad del líder funcional realizar las solicitudes correspondientes mediante los medios definidos anteriormente para el respectivo mantenimiento, que puede ser:

- **Correctivo:** son aquellos cambios precisos para corregir errores del software
  .
- **Evolutivo:** son las novedades, modificaciones y eliminaciones necesarias en un software para cambios en los requerimientos de usuario.

- **Adaptativo**: son las modificaciones que afectan a los entornos en los que el sistema opera, por ejemplo, cambios de configuración del hardware, software de base, base de datos, telecomunicaciones, entre otros.

- **Perfectivo**: son las actividades realizadas para mejorar la calidad interna de los sistemas en cualquiera de los aspectos: remasterización del código, optimización del sistema, rendimiento y/o eficiencia.

2. ESTÁNDARES DE CODIFICACIÓN

2.1 Reglas Para Codificación General

- Para conservar recursos sea muy selectivo en la elección del tipo de dato, asegúrese que el tamaño de una variable no sea excesivamente grande. Por ejemplo en los ciclos *for* es mejor, en la mayoría de las veces utilizar un tipo de dato tipo short que int.
- Mantenga el tiempo de vida de las variables tan corto como sea posible, esto es muy importante por ejemplo cuando se utiliza un recurso finito como una conexión a una Base de Datos.
- Mantenga el *scope*de las variables tan corto como sea posible, esto sirve para evitar confusiones, mejorar la mantenibilidad y además minimiza la dependencia, es decir si por

algún motivo se comete el error de borrar una variable es más fácil de encontrar el error si esta tiene un *scope* más pequeño.

- Use los procedimientos y variables con un solo propósito. Evite crear procedimientos multipropósito que lleven a cabo una variedad de funciones no relacionadas.
- Dentro de una clase, no utilice variables públicas, en cambio utilice procedimientos y propiedades que accedan a dichas variables (privadas), así provee una capa de encapsulación y brinda la posibilidad de validar valores de cambio sobre las mismas, antes de manipularlas directamente.
- Cuando se trabaje en un entorno web distribuido, tenga cuidado de almacenar información en variables de sesión ASP ya que el estado de sesión es almacenado siempre en una sola máquina, considere mejor almacenar dicha información en una base de datos.
- No abra conexiones a datos usando credenciales específicas de usuario, ya que estas no podrán ser reutilizadas por el pool de conexiones.
- Evite el uso de conversión de tipos o casting ya que esto puede generar resultados imprevistos, sobre todo cuando dos variable están involucradas en una sentencia, utilice el cast solo en situaciones triviales, cuando este no sea el caso asegure de comentar la razón por la cual lo hizo.
- Use siempre rutinas de manejo de excepciones
- Sea especifico cuando declare objetos que puedan generar colisión, por ejemplo si tiene dos métodos con el mismo nombre en diferentes *namespaces* escríbalos con el nombre completo incluyendo el del paquete.
- Evite el uso de variables en el ámbito de aplicación (web).
- Use siempre sentencias *Select*-Case o Switch en lugar de utilizar sentencias *if-then* repetitivas.
- Libere explícitamente las referencias a objeto. (variable = nothing ó variable = null)
- Siempre que sea posible utilice polimorfismo en vez de cláusulas Switch o *Select*.

2.2 Nombrado

El esquema de nombres es una de las ayudas más importantes para entender el flujo lógico de una aplicación. Un nombre debe más bien expresar el "qué" que el "cómo". Si se utiliza un nombre que evite referirse a la implementación se estará conservando la abstracción de la estructura ya que la implementación está sujeta a cambios, de esta manera se describe que hace la estructura y no como lo hace.

Por ejemplo es más claro nombrar un procedimiento de acceso a datos SeleccionarRegistro() que RealizarConsultaSelect(), porque lo que importa (para que otra persona entienda el código) es que se supone que hace el método y no como lo hace.

Otra directiva es la de utilizar nombres tan largos como para que se entiendan pero a la vez tan cortos como para que no den información irrelevante, por ejemplo es mejor emplear SeleccionarComida() que SeleccionarlaComidadelMenu().

Desde el punto de vista de la programación, un nombre único sirve solamente para diferenciar un elemento de otro. Los nombres expresivos funcionan como ayuda para el lector, por eso, es lógico dar nombres que sean fáciles de comprender. No obstante, asegúrese de que los nombres escogidos sean compatibles con las reglas de cada lenguaje y con los estándares.

2.3 Utilización De Mayúsculas en la Codificación:

Estilos:

Pascal: primera letra en mayúscula letras de siguientes palabras en mayúscula

BackColor

Camel: primera letra en minúscula letras de siguientes palabras en mayúscula

BackColor

Estructuras (namespaces, procedimientos, clases, interfaces y propiedades)

Los nombres de todas las estructuras de código deben ser en español.

Los namespaces deben empezar por el nombre de la compañía seguido de la unidad de negocio, el producto o proyecto y la funcionalidad:

Dps.FabricaSw.Papelsa.AccesoaDatos

[compañía].[unidad de negocio].[proyecto].[funcionalidad]

- El nombre del ensamblado y el namespace*root* deben ser idénticos
- El nombre de la clase y el archivo fuente deben ser iguales.
- No se debe usar la notación *húngara*, la cual prefija una abreviatura referente al tipo de objeto: lblAceptar (label), btnOK(Botón), etc.
- Evite nombres imprecisos que permitan interpretaciones subjetivas, como por ejemplo *DefinirEsto()*, o bien *ytG8* para una variable. Tales nombres contribuyen más a la ambigüedad que a la abstracción.
- En la POO es redundante incluir nombres de clases en el nombre de las propiedades de clases, como por ejemplo Rectángulo.RectánguloArea, en su lugar, utilice Rectángulo.Area, pues el nombre de la clase ya contiene dicha información.
- Utilice la técnica verbo-sustantivo para nombrar procedimientos que ejecuten alguna operación en un determinado objeto, como por ejemplo CalcularDesperdicio().

- Empiece los nombres de clase y propiedades con un nombre, por ejemplo CuentaBancaria, la primera letra de cada palabra debe ser mayúscula.
- En lenguajes que permitan sobrecarga de funciones, todas las sobrecargas deberían llevar a cabo una función similar. Para los lenguajes que no permitan la sobrecarga de funciones, establezca una nomenclatura estándar relacionada con funciones similares.
- Empiece los nombres de interfaz con el prefijo "I", seguido de un nombre o una frase nominal, como IComponente, o con un adjetivo que describa el comportamiento de la interfaz, como IPersistible. No utilice el subrayado"_"(con la excepción de las variables privadas), y utilice lo menos posible las abreviaturas, ya que pueden causar confusiones.

Clases:

- Use nombres para nombrar clases.
- No utilice el carácter underscore (_).
- Cuando se apropiado utilice una palabra compuesta para referirse a la clase padre de la cual está heredando por ejemplo ApplicationException deriva de Exception esto debe aplicarse solo cuando sea relevante mostrar de que clase está heredando.

  - publicclassFileStream
  - publicclassButton
  - publicclassString
  -

Parámetros:

Use palabras descriptivas para componer el nombre, de forma que este tenga significado en diferentes escenarios, el parámetro debe tener un significado relativo a el método que lo utiliza.

Type GetType(string **typeName**) string Format(string **format**, object[] **args**)

Para el uso de parámetros en scripts de base de datos utilizar antes del nombre del parámetro la consonante p (pNombreParametro)

Métodos:

Utilice verbos o frases con verbos para nombrar los métodos:

- BorrarTodo()
- GetCharArray()
- Invoke()

Eventos:

- Utilice un sufijo EventHandler en eventos handlernames.
- Especifique dos parámetros llamados *sender* y *e*.
- Nombre la clase de los argumentos del evento con el sufijo EventArgs.
- Considere el nombre de los eventos como un verbo, por ejemplo Clicked, Painting.

public delegate void **MouseEventHandler**(object **sender**, MouseEventArgs**e**);

Propiedades:

- Utilice nombres para nombrar las propiedades.
- Debe considerar utilizar en el nombre de la propiedad el tipo de dato utilizado en la propiedad, por ejemplo si se desea retornar el color de fondo de tipo Color creamos una propiedad llamada **BackColor**

```
public class SampleClass
{
public Color BackColor
  {
    // Code for Get and Set accessors goes here.
}
}
```

Variables

- Estas deben nombrarse en minúsculas.
- Es recomendado que las variable booleanas contengan una palabra que describa su estado: puedeEliminarse, esGrande, tieneHijos, etc. Y siempre se debe referir al estado verdadero: tieneCrédito en cambio de noTieneCrédito.
- Incluso para el caso de una variable de poco uso, que deba aparecer sólo en unas cuantas líneas de código, emplee un nombre descriptivo. Utilice nombres de variables de una sola letra, como i o j sólo para índices (ciclos for).
- No utilice números o cadenas literales, como por ejemplo *For i = 1 To 7*. En su lugar, emplee constantes con nombre, del tipo *For i = 1 To Enumeracion.length* para que resulten fáciles de mantener y comprender.

2.4 Base De Datos

Tablas

- Utilice mayúsculas para nombres de tablas.
- Cuando ponga nombres a tablas, hágalo en singular. Por ejemplo, use EMPLEADO en lugar de EMPLEADOS.
- No utilice el carácter (_) para una tabla con nombre compuesto por ejemplo DETALLE_PEDIDO, utilice las dos palabras de forma seguida DETALLEPEDIDO.
- Cuando ponga nombre a las columnas de las tablas, no repita el nombre de la tabla; por ejemplo, evite un campo llamado EstudianteApellido de una tabla llamada Estudiante. (Igual que con las propiedades de una clase).
- No incorpore el tipo de datos en el nombre de una columna.
- Nombre las columnas con notación Camel.

Microsoft SQL Server

- No ponga prefijos sp a los procedimientos almacenados, ya que se trata de un prefijo reservado para la identificación de procedimientos almacenados de sistemas.
- No ponga prefijos *fn_* a las funciones definidas por el usuario, ya que se trata de un prefijo reservado para funciones integradas.
- No ponga prefijos *xp_* a los procedimientos almacenados extendidos, ya que se trata de un prefijo reservado para la identificación de procedimientos almacenados extendidos.

3. GARANTIA Y SOPORTE EN DESARROLLOS CONTRATADOS

Para los desarrollos que son contratados por terceros (proveedores), se deben tener cuenta lo siguiente:

- Garantía mínima y soporte técnico por (6) meses, a partir del recibo a satisfacción, sobre errores de ejecución funcional de los programas que componen el sistema.

- La garantía debe cubrir todo el software, la documentación y los medios que se utilizan para cumplir el objeto del contrato; también en este periodo se debe ofrecer sin costo adicional el soporte y el mantenimiento.

- El proveedor deberá establecerá en forma detallada el procedimiento de solicitud de la garantía y las restricciones de la misma.

- El primer mes de garantía debe ofrecer soporte presencial de al menos una (1) persona de tiempo completo (8 horas diarias) a los usuarios en el uso y operación de la solución y el software, contado a partir de la aceptación.

- El soporte técnico deberá incluir como mínimo soporte telefónico en horario de 8:00 a.m. a 5:00 p.m. de lunes a viernes.

4. RESPONSABILIDADES DE LAS AREAS QUE SOLICITAN DESARROLLOS DE SOFTWARE

- La totalidad de los requerimientos se deben implementar obedeciendo a lo establecido mediante este documento.

- La totalidad de los requerimientos de los sistemas de información deben ser definidos por el área funcional con los instrumentos establecidos para tal fin (Documento de Especificación de Requerimientos de Software - DERS).

- El área funcional deberá realizar las pruebas de aceptación del sistema y deberá establecer el mecanismo para su realización, responsables, documentación y aceptación.

- El área funcional deberá solicitar la puesta en producción de lo implementado una vez lo acepte a entera satisfacción mediante comunicación escrita.

- Para los efectos de trazabilidad de los requerimientos, se debe utilizar la mesa de ayuda o la metodología que se encuentre establecido en ese momento en la Entidad. Aquellas solicitudes que no se registren en la herramienta no serán tramitadas.

- La totalidad de requerimientos, sus modificaciones y adiciones deberán quedar establecidas por escrito, así como la trazabilidad del requerimiento.

- Una vez realizada la reunión de entendimiento y modificado el DERS (si se requiere) queda determinado como documento definitivo y no podrá sufrir modificaciones hasta su puesta en producción. Si se requieren modificaciones, el área funcional deberá solicitar la realización de un nuevo requerimiento o solicitar la no implementación de lo solicitado con la debida justificación.

- En todos los casos aquello solicitado e implementado deberá ser utilizado por el área funcional. No se aceptaran modificaciones (nuevos requerimientos) sobre algo que no se haya puesto en producción o que no haya sido utilizado.
- La totalidad de los requerimientos deberán tener un responsable(el líder funcional) en el área solicitante y se entenderán como el canal oficial de comunicación, no se aceptaran comunicaciones ni observaciones por otros medios, ni de otros funcionarios.

- Los entregables, código, productos o artefactos dentro del desarrollo de software debe estar bajo el control del grupo de infraestructura y en tal sentido las áreas funcionales deben hacer entrega de esta en caso que la tengan.

5. DERECHOS DE AUTOR

La propiedad de todos los derechos de autor y otros derechos de propiedad intelectual con respecto a cualquier recopilación de datos, investigación, hojas de cálculo, gráficos, informes, diseños, productos de trabajo, código de programación, software o cualquier otro documento desarrollados en relación con este contrato ("la propiedad intelectual") será exclusiva del DPS y por lo tanto tendrá todos los derechos de propiedad, aunque el contratista o sus empleados sean los autores. Todo documento relacionado con la propiedad intelectual o conectado de otra manera con este contrato, los servicios u obligaciones deben ser devueltos o entregados al DPS al momento de la terminación del contrato.

Como parte del recibo a satisfacción de los proyectos de software contratados se deberá hacer entrega de código fuente, ejecutables, manuales y la totalidad de lo solicitado. Así como los documentos que en materia de derechos de autor se requieran.

La totalidad de las consideraciones con respecto a los derechos de autor deberán ceñirse y aplicarse de acuerdo a la legislación colombiana y lo que en esta materia conceptué en la Oficina Jurídica del DPS.

Anexo F. planilla control de backups

DPS	CONTROL DE BACKUP	Código: F-TEC-005-CBK
		Fecha de aprobación: 5/04/06
	GIT de Soporte Tecnológico	Versión: 01

01/06/2015

Servidor:	Helike-Euporie-Laomedeia/Halimede-Psamathe-Phoebe/Siarnaq-Tethys
Etiqueta1:	400010000389 - Custodia interna caja fuerte
Label1:	LTO-Backup_BD_156
Etiqueta2:	400010000390 - Custodia externa -- Transcocol
Label2:	LTO-Backup_BD_157

FECHA	SERVIDOR	ESQUEMA DE BD
20/05/2015 25/05/2015 31/05/2015	HELIKE	DQS_MAIN DQS_PROJECTS DQS_STAGING_DATA master MDS MDS_DPS_Auditoria MDS_DPS_Beneficiarios MDS_DPS_Staging_Carga MDS_DPS_Staging_Estandarizacion PDW SSISDB
20/05/2015 25/05/2015 31/05/2015	LAOMEDEIA/HALIMEDE	MapaSocial, MapaSocialStaging, master, SSISDB
20/05/2015 25/05/2015 31/05/2015	PSAMATHE	PROGRAMAS_ANT_DPS, ReportServer, RNEC_Mayores, RNEC_Menores, SISBEN, TablasCruzar, Unidos, Victimas, Generador
20/05/2015 25/05/2015 31/05/2015	PHOEBE/SIARNAQ	BAMArchive, BAMPrimaryImport, BAMStarSchema, BizTalkDTADb, BizTalkMgmtDb, BizTalkMsgBoxDb, BizTalkRuleEngineDb, ESBAdmin, EsbExceptionDb, EsbItineraryDb, GestionInteroperabilidad, Sentinet,
20/05/2015 25/05/2015 31/05/2015	TETHYS	WSS_UsageApplication_backup_2015_05_20_043001_0369 WSS_Content_PortalDPS_backup_2015_05_20_040001_51 WSS_Content_MISitio_backup_2015_05_20_033001_72255 14936ef4478ef175a2_backup_2015_05_20_003000_9903841 365d0a914b988c50d3be72fd14b8_backup_2015_05_20_003000_9903841 17c9e08c2a5df0844c5_backup_2015_05_20_000506_0683900 Search_Ser_App___Intranet_DB_169bb13157b14f389842a53a1d229ec0_backup_2015_05_20_000506_0528165 9b4b6074ece8df7d029_backup_2015_05_20_000506_0528165 c4e465c1104f0baed1d9d4824e732a_backup_2015_05_20_000505_9903264
01/05/2015	FORNJOT	ePO_FORNJOT, tanium, tanium_archive

NOTA: Se hace backup mensual de las bases de datos de los servidores FORNJOT y PRAXIDIKE.

Responsable Luis Alejandro Sánchez Lozano

Anexo G. Fomato solicitud de creación y cancelación de cuentas de usuario

DPS	FORMATO DE SOLICITUD DE CREACIÓN Y CANCELACIÓN DE CUENTAS DE USUARIO	Código:
		Fecha de aprobación:
	GRUPO DE INFRAESTRUCTURA Y SOPORTE DE TI	Versión: 01

FECHA:	dia/mes/año

I. Datos del Responsable de Area que hace la solicitud

Nombre	
Dependencia	
Cargo	
Correo electrónico	

II. Detalles de Cancelación o suspensión de Cuenta de Usuario o derogación de privilegio/perfil

Nombre completo del usuario	
Numero de identificación	
Cargo	

Validez de la solicitud (Marcar con una X)	Indefinida	X	Temporal	

En caso de que sea temporal indicar la duración:		Marcar con una X:		Días
				Meses

Correo electrónico del usuario para la notificación de la cancelación o cambio de permisos:	

III. Sistemas de información sobre los que se solicita la cancelación de cuenta o la derogación del privilegio/perfil

Nombre del sistema de información (Por ejemplo Correo electrónico, Actrea, Orfeo)	Privilegio/Rol de usuario/Perfil de Usuario	Consideraciones adicionales (si aplica)

IV. Evaluación de la Solicitud por parte del Custodio del Sistema de Información

Solicitud cumple con condiciones de seguridad (Marcar con una X)	SI		No	

Razones por las cuales no es aprobada la solicitud (en caso que corresponda)	
1	
2	
3	
4	

Anexo H. Formato de definición de backups de información

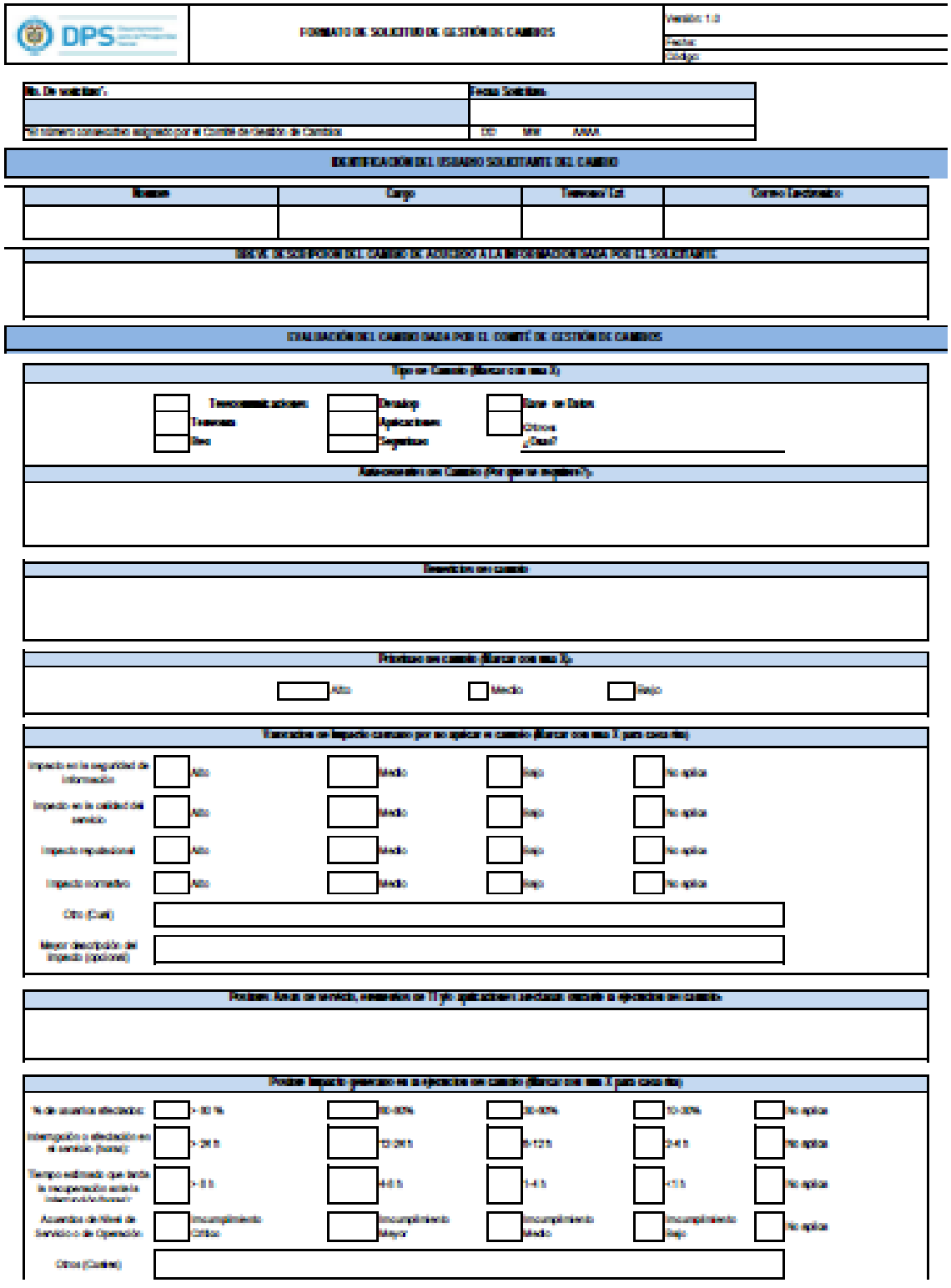
FORMATO DE DEFINICIÓN DE BACKUPS DE INFORMACIÓN

INDICE	SISTEMA DE INFORMACIÓN	SERVIDOR	KEYWORD	RUTA(S) DE LOS ARCHIVOS SOBRE LOS QUE SE REALIZA EL BACKUP	TIPO DE BACKUP	FRECUENCIA DEL BACKUP	PERIODO DE RETENCIÓN	MEDIO DEL ALMACENAMIENTO DEL BACKUP	SITIO DE CUSTODIA	REQUIERE CIFRADO?	
										SI	NO
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						
					Total						

Anexo I. Formato de registro de backups ejecutados

FORMATO DE REGISTRO DE BACKUPS EJECUTADOS														
INDICE	FECHA (DD/MM/AAAA)	HORA (HH:MM:SS)	PERSONA QUE REALIZA EL BACKUP	NOMBRE DEL BACKUP GENERADO (KEYWORD-FECHA-HORA)	SITIO DE ALMACENAMIENTO	BACKUP CIFRADO?		FIRMA	FECHA DE RESTAURACION (DD/MM/AAAA)	PERSONA QUE REALIZA LA RESTAURACIÓN DEL BACKUP	EL BACKUP SE RESTAURO EXITOSAMENTE? (SI aplica)		FIRMA	OBS.
						SI	NO				SI	NO		

Anexo J. Formato solicitud de gestión de cambios



DPS	FORMATO DE SOLICITUD DE GESTIÓN DE CAMBIOS	Versión: 1.0 Fecha: Código:

No. De solicitud*:	Fecha Solicitud:
*El número consecutivo asignado por el Comité de Gestión de Cambios	DD MM AAAA

IDENTIFICACIÓN DEL USUARIO SOLICITANTE DEL CAMBIO

Nombre	Cargo	Teléfono/ Ext.	Correo Electrónico

DESCRIPCIÓN DEL CAMBIO DE ACUERDO A LA INFORMACIÓN DADA POR EL SOLICITANTE

EVALUACIÓN DEL CAMBIO DADA POR EL COMITÉ DE GESTIÓN DE CAMBIOS

Tipo de Cambio (Marcar con una X)

Telecomunicaciones | Desarrollo | Base de Datos
Transporte | Aplicaciones | Otros:
Sitio | Seguridad | ¿Cual?

Antecedentes del Cambio (Por que se requiere?):

Restricciones del cambio

Prioridad del cambio (Marcar con una X):

Alto | Medio | Bajo

Tipos de Impacto esperado por no aplicar el cambio (Marcar con una X para cada fila)

Impacto en la seguridad de información	Alto	Medio	Bajo	No aplica
Impacto en la calidad del servicio	Alto	Medio	Bajo	No aplica
Impacto reputacional	Alto	Medio	Bajo	No aplica
Impacto normativo	Alto	Medio	Bajo	No aplica
Otro (Cual)				
Mayor descripción del impacto (opcional)				

Posibles fallas de servicio, indicadores de TI y/o aplicaciones afectadas durante o ejecución del cambio

Posible impacto generado en la ejecución del cambio (Marcar con una X para cada fila)

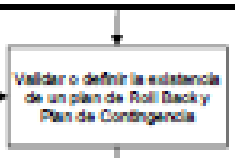
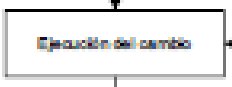
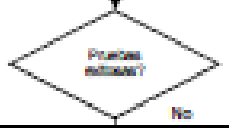
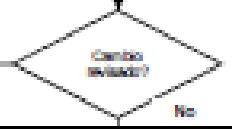
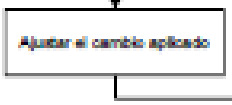
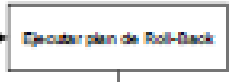
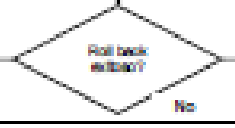
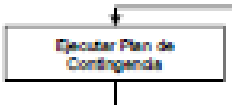
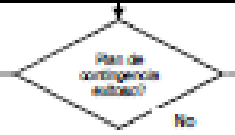
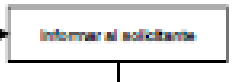
% de usuarios afectados	> 80 %	60-80%	40-60%	10-30%	No aplica
Interrupción o afectación en el servicio (horas)	> 24 h	12-24 h	6-12 h	2-4 h	No aplica
Tiempo estimado que tarda la recuperación ante la materialización del riesgo	> 8 h	4-8 h	1-4 h	<1 h	No aplica
Acuerdos de Nivel de Servicio o de Operación	Incumplimiento Crítico	Incumplimiento Mayor	Incumplimiento Medio	Incumplimiento Bajo	No aplica
Otros (Cuales)					

Anexo K. Formato solicitud de gestión de cambios

DPS	PROCEDIMIENTO DE GESTIÓN DE CAMBIOS	Código:
		FECHA DE APROBACIÓN:
	AREA DE SISTEMAS E INFORMATICA	Versión:01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Recepción de solicitud de gestión de cambio	El proceso de tecnología recibe solicitud a través de la mesa de ayuda, correo electrónico o comunicado escrito.	Solicitud en la mesa de ayuda, correo electrónico o memorando	Coordinador de GIT Infraestructura y Soporte de TI
3	Evaluar la solicitud de gestión de cambio	Evaluar la solicitud de gestión de cambio para determinar la necesidad de aplicar el cambio y si se trata de un cambio normal en la operación o de un cambio de emergencia.	Formato de Solicitud de Gestión de Cambios.	Coordinador de GIT Infraestructura y Soporte de TI
4	Cambio de emergencia? (SI / No)	Si se cumplen las condiciones para un cambio de emergencia se procede a la siguiente actividad de solicitar aprobación para llevar a cabo el cambio de emergencia (actividad 10). Si no se cumplen las condiciones de cambio de emergencia se continua a realizar las actividades normales de planeación del cambio (actividad 5).	Formato de Solicitud de Gestión de Cambios.	Coordinador de GIT Infraestructura y Soporte de TI
5	Convocar al Comité de Gestión de Cambios	Convocar al Comité de Gestión de Cambios conformado por: 1)Custodio del activo sobre el que se aplica el cambio 2)Responsable del activo sobre el que se aplica el cambio 3)Oficial de Seguridad de la información y cualquier Colaborador del DPS que se considere que su presencia es requerida para poder aprobar y planear la ejecución del cambio.	Formato de Solicitud de Gestión de Cambios.	Coordinador de GIT Infraestructura y Soporte de TI
6	Cambio aprobado? (No / SI)	El Comité de Gestión de Cambios debe evaluar la solicitud de cambio a la luz de los beneficios que traerá la aplicación del cambio y también de las posibles afectaciones que se obtendrían al no aplicar el cambio. Dentro de las afectaciones se deben considerar aspectos operacionales, normativos y reputacionales.	Formato de Solicitud de Gestión de Cambios.	Comité de Gestión de Cambios.
7	Realizar la planeación del cambio	El Comité de Gestión de Cambios realiza la definición de la planeación del cambio: ventana de mantenimiento, rollback, pruebas a realizar en un ambiente de pruebas, pruebas a realizar posterior a haber aplicado el cambio en el ambiente de producción y demás aspectos de la planeación. Esta información debe ser consignada en el Formato de Solicitud de Gestión de Cambios.	Formato de Solicitud de Gestión de Cambios.	Comité de Gestión de Cambios.
8	Consultar al propietario del sistema de información por aprobación de una ventana de mantenimiento (en caso de que el cambio genere un evento disruptivo)	Se debe consultar al responsable del proceso propietario del sistema de información para programar una ventana de tiempo que permita la aplicación del cambio sin afectar considerablemente la operación	Email, acta de reunión	Coordinador de GIT Infraestructura y Soporte de TI Responsable/Custodio del sistema de información
9	Verificar el cambio en un entorno de pruebas	En caso de que en la planeación de haya determinado la necesidad de aplicar ciertas pruebas en un ambiente de pruebas antes de ejecutar el cambio en producción, se deberá programar y realizar esta actividad.	Formato de Solicitud de Gestión de Cambios.	Coordinador de GIT Infraestructura y Soporte de TI Responsable/Custodio del sistema de información

DPS Departamento para la Prosperidad Social	PROCEDIMIENTO DE GESTIÓN DE CAMBIOS	Código:
		Fecha de aprobación:
	ÁREA DE SISTEMAS E INFORMÁTICA	Versión:01

10		Se debe verificar que exista un mecanismo de Roll-back que permita la vuelta del activo al estado anterior en caso que de que la aplicación del cambio sobre el activo no resulte como se esperaba. Adicionalmente se debe validar que haya un plan de contingencia para situaciones en las cuales el activo quede inoperante (y la ejecución del Roll-back no sea exitosa). Generalmente el plan de contingencia hace referencia a un procedimiento de recuperación ante desastres (DRP), pero si no existe dicho procedimiento de recuperación se debe considerar cual sería el plan de contingencia.	Formato de Solicitud de Gestión de Cambios	Coordinador de GIT Infraestructura y Soporte de TI Responsable/Custodio del sistema de información
11		Ejecutar el cambio de acuerdo a las especifica definidas previamente	Cambio ejecutado sobre el sistema	Responsable/Custodio del sistema de información
12		Se debe validar la aplicación exitosa del cambio de acuerdo a los criterios de aceptación definidos en la planeación del cambio (actividad 5)	Formato de Solicitud de Gestión de Cambios	Responsable/Custodio del sistema de información
13		Si el cambio falló y no ha sido revisado con anterioridad, se procederá a revisarlo (actividad 14). Si el cambio ya fue revisado y no se lograron unas pruebas exitosas se procede a aplicar el plan de Roll back (actividad 15)	Formato de Solicitud de Gestión de Cambios	Responsable/Custodio del sistema de información
14		Validar la posibilidad de ajustar el cambio aplicado sin que se supere la ventana de tiempo acordada	Cambio ajustado sobre el sistema	Responsable/Custodio del sistema de información
15		Ejecutar el plan de roll back para restaurar el activo al estado anterior a la aplicación del cambio	Cambio ajustado sobre el sistema	Responsable/Custodio del sistema de información
16		Validar que el activo y sus servicios asociados se encuentren funcionales y con las mismas prestaciones existentes antes de haber aplicado el cambio	Formato de Solicitud de Gestión de Cambios	Responsable/Custodio del sistema de información
17		Ejecutar el plan de contingencia definido previamente para cumplir con las variables de recuperación (si se encuentran definidas) o con la ventana de tiempo acordada	Contingencia ejecutada	Responsable/Custodio del sistema de información
18		Validar que la estrategia de recuperación haya sido exitosa. Esto incluye la recuperación, restauración y normalización del servicio.	Formato de Solicitud de Gestión de Cambios	Responsable/Custodio del sistema de información
19		Informar al usuario solicitante sobre el resultado de la gestión del cambio indicando tanto una situación de ejecución exitosa como una situación de error. En el caso de error se debe informar la situación de error obtenida para que el solicitante considere un replanteamiento del cambio	Email, Acta de reunión	Responsable/Custodio del sistema de información
20				

Anexo L. Control de ingreso al centro de cómputo

	CONTROL DE INGRESO AL CENTRO DE CÓMPUTO	Versión: 1.0 Fecha: 23/12/2013 Código: GT-F-09

Nombre Funcionario y/o Contratista	Fecha	Hora de Entrada	Hora de Salida	Actividad	Servidor No. de Rack y/o Aplicativo al que Accedió	Nombre Acompañante y/o Acompañantes	Firma

Anexo M. Procedimiento de cancelación de cuentas de usuario

	PROCEDIMIENTO DE CANCELACIÓN DE CUENTAS DE USUARIO	Código:
DPS		Fecha de aprobación:
	AREA DE SISTEMAS E INFORMATICA	Versión:01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Recepción de solicitud	El proceso de tecnología recibe solicitud a través de la mesa de ayuda, correo electrónico o memorando.	Solicitud en la mesa de ayuda, memorando o correo electrónico que incluye el Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Corresponde a la persona responsable del area a la cual pertenece el usuario para el cual se solicita la cancelación de una cuenta de usuario o la derogación de un rol o privilegio. Puede ser el Jefe de la Oficina, Coordinador, Director, o quien ellos deleguen.
3	Validación de las condiciones para la cancelación de cuentas de usuario y/o derogación de privilegios	Validar la condiciones de seguridad. -Se debe cumplir la condición de segregación de funciones (una actividad crítica no puede quedar a cargo de un unico usuario). Si no se cumple esta condición se debe indicar al solicitante que antes de solicitar la cancelación de una cuenta o la derogación de un privilegio para un usuario X, primero se debe indicar a un usuario Y a la cual se le otorgarán los privilegios que se revoquen al usuario X.	Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Custodio del sistema de información
4	No Se cumplen las condiciones? Si	Si se cumplen las condiciones se procede a cancelar la cuenta de usuario o a derogar los privilegios. Si no se cumplen las condiciones se debe informar al solicitante indicando las razones para no proceder a procesar el permiso.	Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Custodio del sistema de información
5	Cancelación de cuenta de usuario y/o derogación de privilegios	Cancelar la cuenta de usuario o derogar el privelegio indicado en la solicitud	Registro de actividad en el gestor de autenticación y autorización propio del sistema de información	Custodio del sistema de información
6	Enviar notificación al solicitante	Notificar al solicitante y al usuario del resultado de la solicitud. En caso de que la solicitud no haya sido posible, se debe informar al solicitante la razón por medio del Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario.	Actualización en la mesa de ayuda, correo electrónico o memorando incluyendo el Formato de Solicitud de Creación y Cancelación de Cuentas de Usuario	Personal de Soporte
	Final			

Anexo N. Procedimiento de ejecución de backups

DPS Departamento para la Prosperidad Social	PROCEDIMIENTO DE EJECUCION DE BACKUPS	Código:
		Fecha de aprobación:
	AREA DE SISTEMAS E INFORMATICA	Versión:01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	SI / No: Características del Backup definidas?	Si se encuentran definidas las características del backup se procede a realizar la ejecución del mismo (Actividad 5). Si no se encuentran definidas las características del backup se procede a solicitar al Oficial de Seguridad de la Información la definición.	Email	Responsable/Custodio del sistema de información
3	Definición de las características del backup (Formato Definición Backups de Información)	Se define en el Formato de Definición Backups las características: Tipo (incremental, total, diferencial, etc), frecuencia (diario, semanal, mensual, etc), medio de almacenamiento, lugar de custodia, etc.	Formato de Definicion de Backups de Información	Oficial de Seguridad de la Información, DBA
4	Configuración del backup	Realizar la configuración del backup de acuerdo a las características definidas en la actividad 2	Backup configurado en el aplicativo de generación de backups	Responsable/Custodio del sistema de información
5	Ejecución del backup	Ejecutar el backup. Se realiza manualmente la primera ocasión para garantizar una correcta configuración. Posteriormente se puede ejecutar de forma automática de acuerdo a la frecuencia definida.	Ficheros resultantes del backup	Responsable/Custodio del sistema de información
6	SI / Backup exitoso? / No	Validar la ejecución sin errores del backup. Si el backup se ejecuto exitosamente se procede a registrar el backup en el formato de Reagistro de Backups (Actividad 8). Si el backup falló se debe hacer una revisión de la configuración del backup, de la ruta de destino donde se almacena el backup, y demas aspectos que pueden generar la falla.	Formato de Registro de Backups Ejecutados	Responsable/Custodio del sistema de información
7	Revisar y ajustar condiciones del backup	Si el backup falló se debe hacer una revisión y ajuste de la configuración del backup, de la ruta de destino donde se almacena el backup, y de los demas aspectos que de acuerdo al error generado den indicio de la causa de la falla.	Backup configurado en el aplicativo de generación de backups	Responsable/Custodio del sistema de información
8	Registro del backup ejecutado (Formato de Registro de Backups Ejecutados)	El proceso de tecnología recibe solicitud a través de la mesa de ayuda, correo electrónico o comunicado escrito.	Formato de Registro de Backups Ejecutados	Responsable/Custodio del sistema de información
9	Disposición del medio de almacenamiento	Se debe disponer el medio de almacenamiento que contiene el backup en el lugar definido de acuerdo al Formato de Registro de Backups de Información	Formato de Registro de Backups Ejecutados	Responsable/Custodio del sistema de información
10	Final			

Anexo O. Procedimiento de restauración de backups

	PROCEDIMIENTO DE RESTAURACIÓN DE BACKUPS	Código:
DPS Departamento para la Prosperidad Social		Fecha de aprobación:
	AREA DE SISTEMAS E INFORMATICA	Versión:01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Selección aleatoria de un backup	Seleccionar aleatoriamente un backup de los incluidos en el Formato de Registro de Backups Ejecutados	Formato de Registro de Backups Ejecutados	Responsable/Custodio del sistema de información
3	Realizar la restauración del backup	Restaurar el backup por medio del aplicativo de recuperación. Utilizar la contraseña de cifrado en caso de ser necesario.	Formato de Registro de Backups Ejecutados	Responsable/Custodio del sistema de información
4	Backup restaurado exitosamente? (Si / No)	Validar que el backup haya sido restaurado exitosamente	Formato de Registro de Backups Ejecutados	Responsable/Custodio del sistema de información
5	Reportar el evento como un Incidente de seguridad de la información	Si el backup no se restauró exitosamente se debe reportar la situación mediante un incidente de seguridad de la información	Ficheros del Backup restaurado	Responsable/Custodio del sistema de información
6	Registro de la restauración del backup en el Formato de Registro de Backups ejecutados	El resultado de la restauración se debe registrar en el Formato de Registro de Backups Ejecutados	Formato de Registro de Backups Ejecutados	Responsable/Custodio del sistema de información
10	Final			

Anexo P. Procedimiento de entrega de base de datos

DPS	PROCEDIMIENTO DE ENTREGA DE BASES DE DATOS	Código:
		Fecha de aprobación:
	ÁREA: SISTEMAS E INFORMÁTICA	Versión: 01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Recepción de la solicitud para el respectivo trámite	Recibir la solicitud de entrega de bases de datos por parte del solicitante y remitirla al coordinador del área de seguimiento del Nivel Nacional. Para información asociada a la Dirección de Ingreso Social aplican los siguientes criterios: a) Si la solicitud viene de parte de una Institución de educación superior o un centro de investigación, remitirla al coordinador del GT Estudios Técnicos. b) Si la solicitud viene de parte de un Ente de Control, remitirla al coordinador del área de Seguimiento del Nivel Nacional. c) Si la solicitud viene de parte de una Entidad de la Rama Ejecutiva, remitirla al coordinador del área de Seguimiento del Nivel Nacional. d) Si la solicitud viene por orden judicial, remitirla al coordinador del Grupo de Trabajo Antifraudes.	Solicitud por medio físico o virtual	Colaboradores del Nivel Nacional y Departamental
3	Análisis de la solicitud de entrega de la base de datos	Analizar la solicitud considerando mínimo los siguientes aspectos: a)Solicitante (Entidad del sector público o privada) b)Información solicitada (Conjunto de campos) c)Nivel de clasificación para cada uno de los campos solicitados (Se debe mirar el nivel de clasificación correspondiente del Registro de Inventario de Información) d)Fines para los cuales se solicita la información (En caso de que se indique en la solicitud). e)Existencia de un convenio o contrato interadministrativo. Estos aspectos permitirán determinar si es viable la entrega de información de acuerdo a la normatividad vigente.		Coordinador/Responsable del programa
4	Si La solicitud de información es No	Si el resultado del análisis determina que es viable la entrega de la base de datos, pasar al punto 7. De lo contrario, continuar en la siguiente actividad.		Coordinador
5	Emisión de respuesta	Emitir respuesta al solicitante por medio escrito indicando las razones por las cuales no se entregará la base de datos. Considerar la aplicación de la Ley 1712 de 2014 para redactar la respuesta.	Correo electrónico/memorando	Coordinador
6	Fin			
7	Generación de los datos	Obtener el conjunto de datos solicitados	Registro de actividad en el sistema de información o carpeta digital	Coordinador

Anexo Q. Procedimiento de gestión de cambios

DPS	PROCEDIMIENTO DE GESTIÓN DE CAMBIOS	Código:
		Fecha de aprobación:
	AREA DE SISTEMAS E INFORMATICA	Versión:01

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Recepción de solicitud de gestión de cambio	El proceso de tecnología recibe solicitud a través de la mesa de ayuda, correo electrónico o comunicado escrito.	Solicitud en la mesa de ayuda, correo electrónico o memorando	Coordinador de GIT Infraestructura y Soporte de TI
3	Evaluar la solicitud de gestión de cambio	Evaluar la solicitud de gestión de cambio para determinar la necesidad de aplicar el cambio y si se trata de un cambio normal en la operación o de un cambio de emergencia.	Formato de Solicitud de Gestión de Cambios	Coordinador de GIT Infraestructura y Soporte de TI
4	Cambio de emergencia? (Si / No)	Si se cumplen las condiciones para un cambio de emergencia se procede a la siguiente actividad de solicitar aprobación para llevar a cabo el cambio de emergencia (actividad 10). Si no se cumplen las condiciones de cambio de emergencia se continua a realizar las actividades normales de planeación del cambio (actividad 5).	Formato de Solicitud de Gestión de Cambios	Coordinador de GIT Infraestructura y Soporte de TI
5	Convocar al Comite de Gestión de Cambios	Convocar al Comité de Gestión de Cambios conformado por: 1)Custodio del activo sobre el que se aplica el cambio 2)Responsable del activo sobre el que se aplica el cambio 3)Oficial de Seguridad de la información y cualquier Colaborador del DPS que se considere que su presencia es requerida para poder aprobar y planear la ejecución del cambio.	Formato de Solicitud de Gestión de Cambios	Coordinador de GIT Infraestructura y Soporte de TI
6	Cambio aprobado? (No / Si)	El Comité de Gestión de Cambios debe evaluar la solicitud de cambio a la luz de los beneficios que trae la aplicación del cambio y también de las posibles afectaciones que se obtendrían si no aplicar el cambio. Dentro de las afectaciones se deben considerar aspectos operacionales, normativos y reputacionales.	Formato de Solicitud de Gestión de Cambios	Comité de Gestión de Cambios
7	Realizar la planeación del cambio	El Comité de Gestión de Cambios realiza la definición de la planeación del cambio: ventana de mantenimiento, rollback, pruebas a realizar en un ambiente de pruebas, pruebas a realizar posterior a haber aplicado el cambio en el ambiente de producción y demas aspectos de la planeación. Esta información debe ser consignada en el Formato de Solicitud de Gestion de Cambios.	Formato de Solicitud de Gestión de Cambios	Comité de Gestión de Cambios
8	Consultar al propietario del sistema de información por aprobación de una ventana de mantenimiento (en caso de que el cambio genere un evento disruptivo)	Se debe consultar al responsable del proceso propietario del sistema de información para programar una ventana de tiempo que permita la aplicación del cambio sin afectar considerablemente la operación	Email, acta de reunión	Coordinador de GIT Infraestructura y Soporte de TI Responsable/Custodio del sistema de información
9	Verificar el cambio en un entorno de pruebas	En caso de que en la planeación de haya determinado la necesidad de aplicar ciertas pruebas en un ambiente de pruebas antes de ejecutar el cambio en producción, se deberá programar y realizar esta actividad.	Formato de Solicitud de Gestión de Cambios	Coordinador de GIT Infraestructura y Soporte de TI Responsable/Custodio del sistema de información

Anexo R. Procedimiento implementación de requerimientos en las bases de datos

DPS	Procedimiento de Implementacion de Requerimientos en las BD	Código:
		Fecha de aprobación:
	PROCESO: GT de Soporte Tecnológico	

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Recibo de solicitud	Recepción de la solicitud generada por la mesa de ayuda,Correo electrónico, etc.	Mesa de ayuda o Correo electrónico.	Ing. Desarrollo del programa
3	Análisis solicitud	Se analiza la solicitud efectuada por el Ing de desarrollo	Mesa de ayuda o Correo electrónico.	Administrador Base de Datos
4	Es viable la implementación (NO)	De acuerdo con el análisis, se determina la viabilidad de la implementación	Mesa de ayuda o Correo electrónico.	Administrador Base de Datos
5	Se ejecutan el script o los scripts en la BD	Se ejecutan los scripts en la Base de Datos	Mesa de ayuda o Correo electrónico.	Administrador Base de Datos
6	La ejecucion de los script es (SI / NO)	Los requerimientos enviados se ejecutan correctamente o parcialmente de ser asi de devuelven para su correcion	Mesa de ayuda o Correo electrónico.	Administrador Base de Datos
7	Se envia reporte de los errores generados al Ing. de desarrollo	Se reportan los errores que se generan	Mesa de ayuda o Correo electrónico.	Administrador Base de Datos
8	El Ing. de Desarrollo hace las correciones pertinentes y envia de nuevo el script o	Se hace las correciones necesarias y se reciben para ser ejecutadas de nuevo	Mesa de ayuda o Correo electrónico.	Ing. Desarrollo del programa
9	La correcion enviada es satisfactoria (NO / SI)	Se ejecuta de nuevo los scripts de salir error se devuelven para su correcion	Mesa de ayuda o Correo electrónico.	Administrador Base de Datos
10	Se llena el reporte en la mesa de ayuda o se responde correo electronico	Se llena el reporte final y se cierra el ticket de la mesa de ayuda	Mesa de ayuda o Correo electrónico.	Administrador Base de Datos
11	Fin			

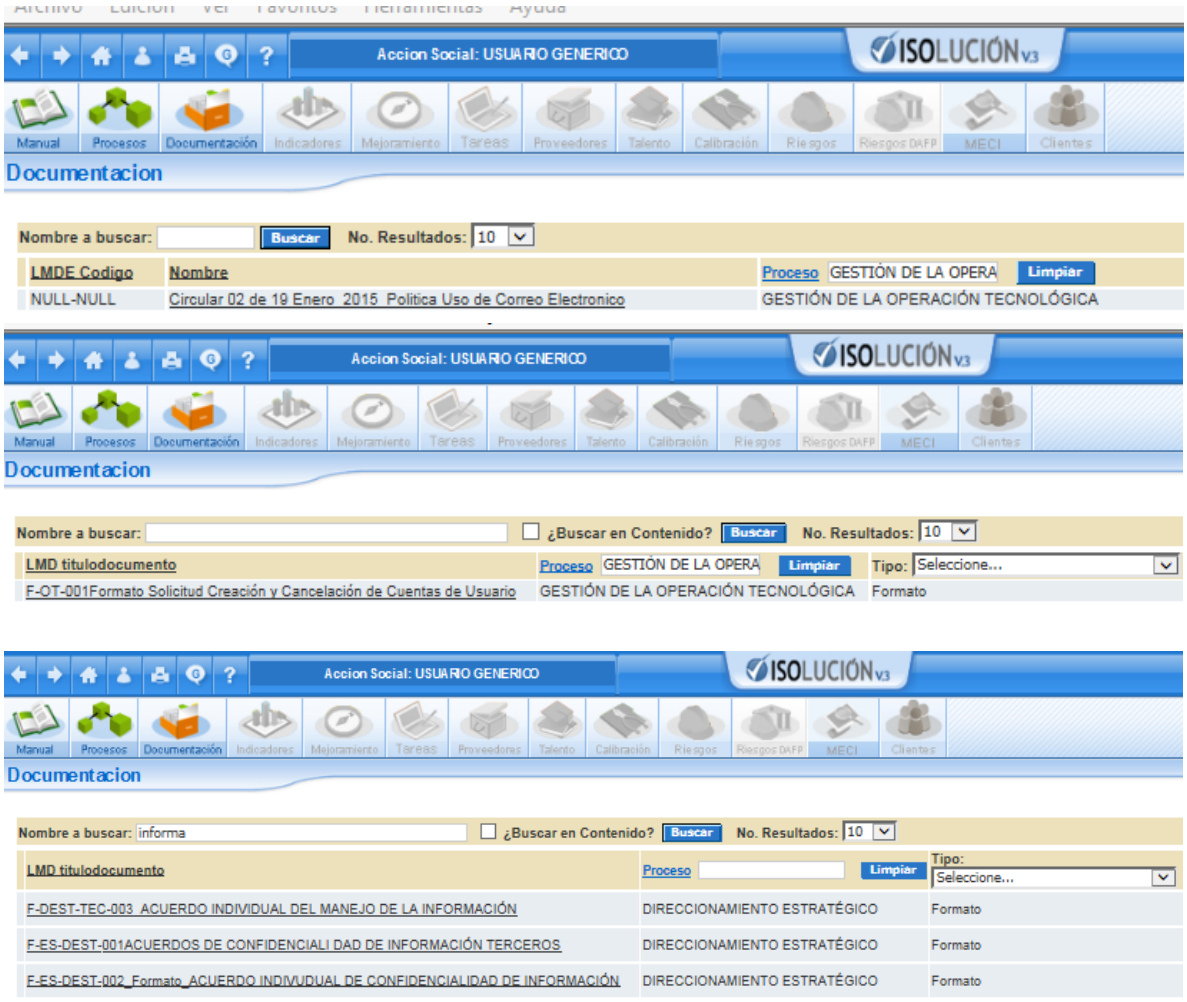
Anexo S. ProcedimientoNotificaciónde eventosygestiónde incidentesdeseguridad

DPS	PROCEDIMIENTO DE NOTIFICACIÓN DE EVENTOS Y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		Código:	
			Fecha de aprobación:	
	ÁREA DE SISTEMAS E INFORMÁTICA		Versión:	

No.	ACTIVIDAD	DESCRIPCIÓN	REGISTRO	RESPONSABLE
1	Inicio			
2	Notificar eventos de seguridad	Cualquier usuario puede reportar un evento de seguridad a través de cualquiera de los siguientes canales autorizados: 1) Correo electrónico (dirigido al email del coordinador del GT de Infraestructura y Soporte de TI y/o al correo seguridaddelainformacion@dps.gov.co 2) Ticket en la mesa de ayuda 3) Memorando (dirigido al coordinador del GT de Infraestructura y Soporte de TI)	Ticket en la Mesa de ayuda, correo electrónico, memorando	Usuario
3	Evaluar el evento reportado	Comunicarse con el usuario quien informó del evento para ampliar la información. Clasificar, diagnosticar y evaluar el evento de seguridad en términos de Impacto (Afectación de Datos). Producto de esta valoración se determina si efectivamente se trata de un evento de seguridad o debe ser considerado como un incidente de seguridad de la información	Formato de Gestión de Incidentes de Seguridad	Oficial de Seguridad
4	¿Es un evento? (No / Sí)	Si la notificación es un evento continua, en caso contrario (es un incidente) vaya al paso 10	Formato de Gestión de Incidentes de Seguridad	Oficial de Seguridad
5	Resolución del evento	Determinar las acciones pertinentes para evitar que el evento de seguridad vuelva a ocurrir	Formato de Gestión de Incidentes de Seguridad	Oficial de Seguridad
6	Aplicar las acciones para la resolución del evento	Realizar actividades tendientes a solucionar el evento, definir acciones correctivas y preventivas según corresponda	Formato de Gestión de Incidentes de Seguridad	Oficial de Seguridad/Oficinas proceso afectado/procesos de apoyo
7	Informar al usuario la solución aplicada	Enviar informe vía correo electrónico al usuario que notificó el evento	Formato de Gestión de Incidentes de Seguridad	Oficial de Seguridad
8	Cerrar solicitud	Cerrar el reporte de evento	Ticket/Mesa de ayuda, correo, memorando	Oficial de Seguridad
9	Final			
10	Aplicar cadena de custodia administrativa	Aplicar cadena de custodia administrativa para asegurar que las evidencias sean válidas y probatorias	Formato de Gestión de Incidentes de Seguridad	Oficial de Seguridad
11	Determinar la resolución al incidente	De acuerdo a la escala de clasificación y los pilares de seguridad de la información (integridad, confidencialidad y disponibilidad) determinar que ajustes se deben hacer sobre los controles o políticas de seguridad existentes ya sea la aplicación de nuevos controles o políticas	Formato de Gestión de Incidentes de Seguridad	Oficial de Seguridad/Oficinas proceso afectado/Coordinador del GT Infraestructura y Soporte de TI
12	Aplicar las acciones para la resolución del incidente	Realizar actividades tendientes a resolver el incidente de seguridad de la información. Definir acciones correctivas y preventivas según corresponda	Formato de Gestión de Incidentes de Seguridad	Coordinador del GT Infraestructura y Soporte de TI/Oficial de Seguridad/Oficinas proceso afectado/procesos de apoyo
13	Notificar a la Oficina Asesora Jurídica con presentación de evidencia	Informar a la Oficina Asesora Jurídica el reporte del incidente y adjuntar la evidencia recopilada	Memorando o correo electrónico incluyendo el Formato de Gestión de Incidentes de Seguridad	Coordinador del GT Infraestructura y Soporte de TI
14	Informar al Comité de TI	Generar un reporte del consolidado de los incidentes de seguridad para el comité de TI del DPS, el cual tiene dentro de sus funciones la revisión de aspectos de seguridad de la información.	Informe, acta adjunta Formato de Gestión de Incidentes de Seguridad	Coordinador del GT Infraestructura y Soporte de TI/Oficial de Seguridad
15	Final			

Anexo T. Documentos publicados

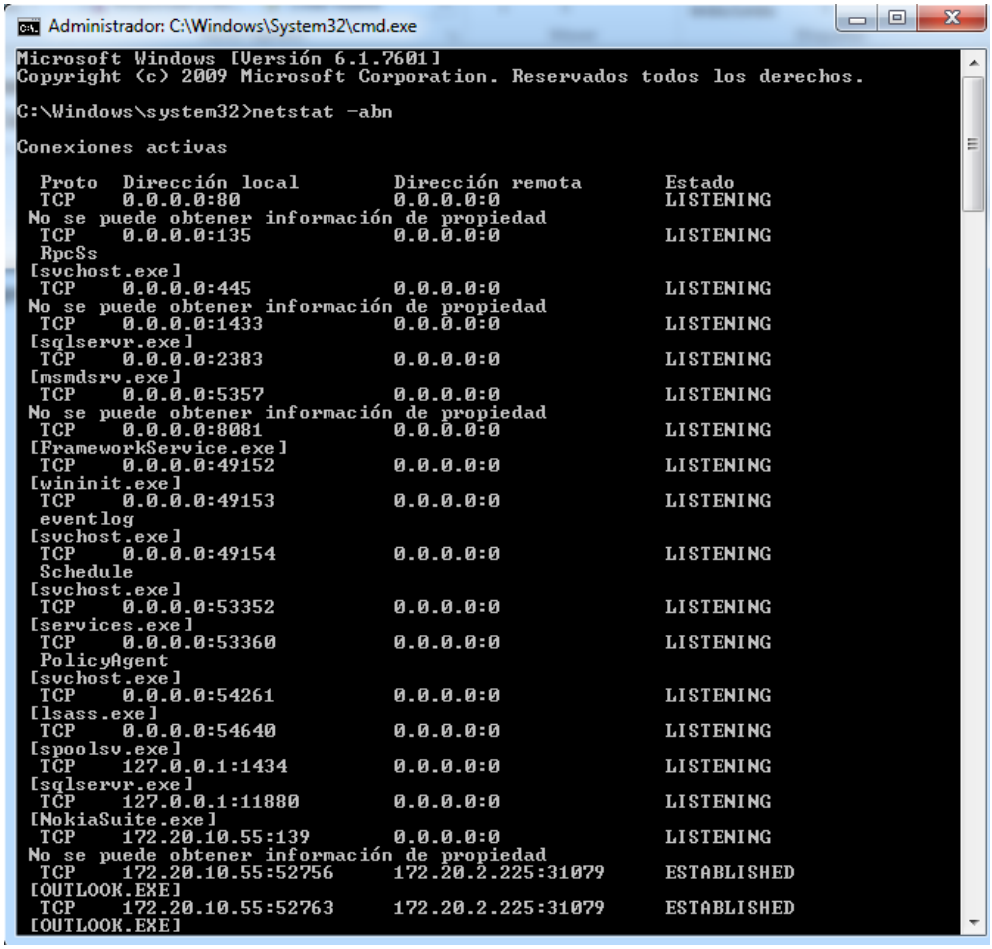
Figura 2. Documentos publicados



Fuente: Intranet Departamento para la Prosperidad Social - DPS

Anexo U. Puertos habilitados

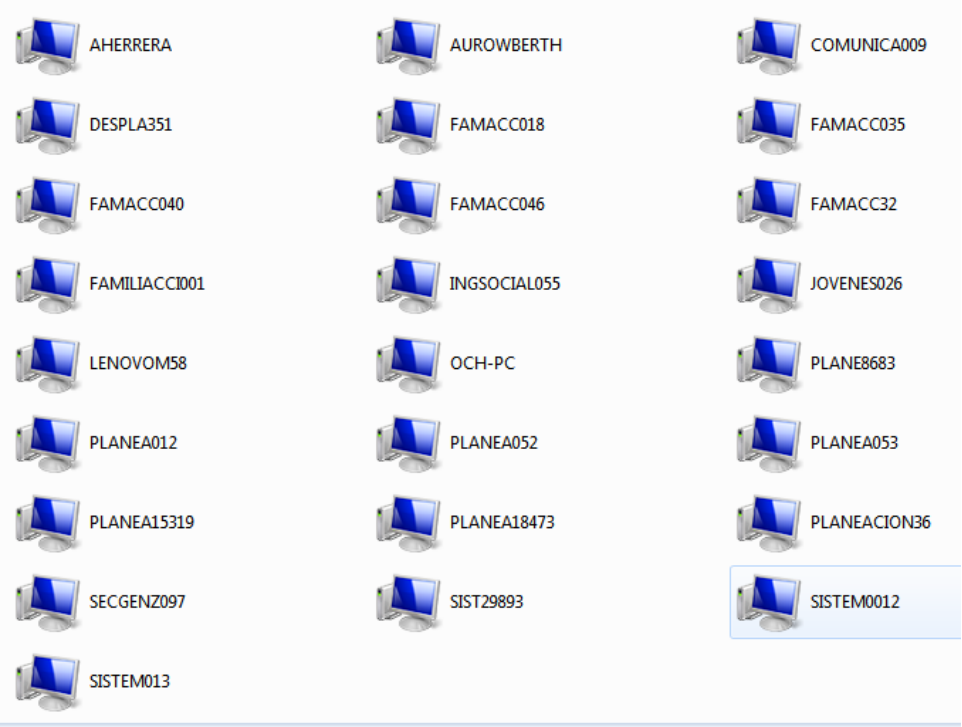
Figura 3. Puertos habilitados



Fuente: Autor

Anexo V. Nombres de equipos por segmento de red

Figura 4. Nombres de equipos por segmento de red



Fuente: Autor