República de Colombia
Ministerio de Hacienda y Crédito Público
Supersolidaria
Superintendencia de la Economía Solidaria

MINHACIENDA
TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

Catálogo de Servicios de TI críticos

Oficina Asesora de Planeación y Sistemas

Bogotá, Diciembre de 2017

"Supervisión para el crecimiento social
y económico del sector solidario"

Contenido

INTRODUCCIÓN

El catálogo de servicios de tecnologías de la información - TI críticos, se constituye en una de las principales herramientas de la gestión estratégica de TI. Por medio de éste se da a conocer el conjunto de servicios de TI que opera la Superintendencia de a Economía Solidaria y que tienen incidencia en la operación toda vez que se consideran críticos y que pueden afectar la continuidad del negocio si no se les realiza el debido tratamiento y seguimiento.

En busca de ofrecer un servicio con calidad, la Oficina Asesora de Planeación y Sistemas, dirige sus esfuerzos en la optimización de sus actividades y organización para la implementación, entrega y soporte de los servicios de Tecnología de Información y Comunicaciones que generan valor a la Superintendencia de la Economía Solidaria – Supersolidaria.

El proceso de definición y actualización del Catálogo de Servicios de TI críticos empieza cuando se detecta una oportunidad de servicio de TI que debe tener un tratamiento especial debido a su nivel de importancia y/o criticidad para la entidad.

1. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Amenaza Externa: Amenaza que se origina fuera de una organización.

Amenaza Interna: Amenaza que se origina en una organización.

Análisis de Riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

Arquitectura abierta de red: Es el conjunto de características técnicas de las redes de telecomunicaciones que les permite interconectarse entre sí a nivel físico y lógico, de tal manera que exista interoperabilidad entre ellas. (Decreto 2870 de 2007, Artículo 2º).

Ataques multi-etapas: Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.

Ataques Web: Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Autorización: Acto administrativo mediante el cual se faculta a un concesionario para establecer, modificar, ensanchar, renovar, ampliar o expandir las características iniciales establecidas para las redes y los sistemas de telecomunicaciones o para la prestación de servicios o el desarrollo de actividades de telecomunicaciones.

Cancelación: Es el acto administrativo mediante el cual se da por terminada la autorización, el permiso o la concesión, ya sea por el vencimiento del término de la concesión o bien, a solicitud de parte, o como consecuencia de una investigación administrativa en la cual se imponga el tipo de sanción de cancelación.

Conectividad: Modelo de cofinanciación en el que participen constructores, beneficiaros VIS, prestadores de servicios de Internet, y el Estado.

Confidencialidad: Propiedad de la información que determina que esté disponible a personas autorizadas.

Conjunto de Datos: Es un conjunto de variables y datos asociados.

Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Firewall: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Front Office: Es el lugar donde el usuario entra en contacto con la entidad y se refiere al conjunto de estructuras que gestionan la interacción con dicho ciudadano o usuario.

Gobierno en Línea (GEL): Es una estrategia liderada por el Ministerio de Tecnologías de la Información y Comunicaciones, es el conjunto de instrumentos técnicos, normativos y de política pública que promueven la construcción de un Estado más eficiente, transparente y participativo, y que a su vez, preste mejores servicios con la colaboración de toda la sociedad mediante el aprovechamiento de la tecnología.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

Registro: Información de fecha, hora, destinatario y consecutivo que se asigna a través del Sistema de Gestión Documental, a las respuestas generadas para las PQR y Derechos de Petición.

Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.

Servicio en Línea: Servicio que puede ser prestado por medios electrónicos a través del portal de una entidad.

Tecnologías de la Información (TI): Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

Tecnologías de la Información y las Comunicaciones (TIC): Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

Trámite en Línea: Trámite que puede ser realizado por medios electrónicos a través del portal de una entidad, ya sea de manera parcial, en alguno de sus pasos o etapas, o total, hasta obtener completamente el resultado requerido.

Usabilidad: La usabilidad es un atributo relacionado con la facilidad de uso. Más específicamente, se refiere a la rapidez con que se puede aprender a utilizar algo, la eficiencia al utilizarlo, cuán memorable es, cuál es su grado de propensión al error, y cuánto le gusta a los usuarios. Si una característica no se puede utilizar o no se utiliza es como si no existiera. (Nielsen)

Usuario (UIT-T Rec M.60 (93)): Persona o máquina delegada por un cliente para utilizar los servicios y/o facilidades de una red de telecomunicaciones. En el contexto de los servicios de telecomunicación: un ser humano que utiliza un servicio. En un contexto técnico: un ser humano, una entidad o un proceso. Nota - Un usuario no será necesariamente un abonado a un servicio de telecomunicación. F.500 (92), H.101.

2. PRIORIZACIÓN DE UN INCIDENTE Vs SERVICIO DE TI CRÍTICO

Normalmente la prioridad de un incidente en un Servicio TI crítico se define en función de:

- Urgencia: Cuán rápido el negocio necesita una solución.
- El impacto: Generalmente medido con la cantidad de usuarios afectados por el

Otros factores determinantes del nivel de impacto son:

- Riesgo de vida.
- Número de servicios afectados.
- Nivel de pérdidas financieras.
- Efectos en la imagen (reputación) del negocio.
- Violación de marcos legales o regulatorios.

3. NIVEL DE CRITICIDAD Y PRIORIZACIÓN DEL IMPACTO

		Imapcto		
		Alto	Medio	Bajo
Urgencia	Alta	1	2	3
	Media	2	3	4
	Baja	3	4	5

Código de prioridad	Descripción	Tiempo de resolución promedio
1	Críitica	1 hora
2	Alta	8 horas
3	Media	24 horas
4	Baja	48 horas
5	Planificada	Planificada

4. RESOLUCIÓN Y RECUPERACIÓN

Involucra la resolución del incidente para lo cual se pueden usar los siguientes métodos:

- Realizarlo conjuntamente con el usuario. (Usuario)
- Resolverlo remotamente. (Remotamente)
- Utilizando un grupo de soporte presencial. (Soporte)
- Contactando un proveedor externo. (Proveedor)

5. TRATAMIENTO DE LOS SERVICIOS DE TI CRÍTICOS EN LA SUPERSOLIDARIA

Nombre del Servicio:	***Servidor de dominio***
Objetivo:	Los Servicios del directorio activo o Active Directory (AD DS) son un sistema que proporciona funciones como la autenticación de todos los usuarios y los equipos de cómputo sobre la red de datos de la entidad, la aplicación de configuración de directivas y la administración centralizada de usuarios y equipos. Este equipo además es el responsable de la resolución de nombres DHCP sobre el dominio principal y las aplicaciones al interior de la entidad, también controla y da salida a internet mediante los WIN, de igual manera trabaja en conjunto con el firewall resolviendo el dominio tanto interno como externo, haciendo la entidad visible desde el exterior.
Descripción:	Dentro de la infraestructura del centro de cómputo existen elementos los cuales son de una altísima criticidad entre ellos encontramos el servidor de dominio, el cual está montado sobre una maquina marca Hp modelo HP ProLiant DL160 G6. Este elemento ubicado en el centro de cómputo del piso 16, y como se había mencionado antes, permite la operación de todos los servicios de red, autenticación de usuarios, de equipos y servidores, resolución de nombres y de ips de las maquinas, así mismo que la interacción con el firewall y la aplicación de políticas y reglas establecidas por la O.A.P.S.
Necesidades que satisface:	Todos los servicios de red, autenticación y seguridad de la superintendencia de la economía solidaria.
Responsable del Servicio:	Oficina asesora de planeación y sistemas. ext 10152
Políticas:	No se tienen establecidas políticas sobre este elemento.
Seguridad:	1. Seguridad perimetral de control acceso al centro de computo 2. Equipo con password de administrador. 3. Control y restricción de usuarios que manipulan este equipo 4. Auditoria sobre el log de eventos para la verificación de las acciones tomadas sobre este equipo. 5. Backup de respaldo para la restauración de la máquina.

	6.
Características de la falla:	1. Daño físico sobre el servidor 2. Des-configuración 3. Virus
Impacto:	1
Código de prioridad:	1
Resolución y Recuperación:	Reconfiguración de equipo. Intercambio de discos duros con otro servidor de mismas características. Intercambio de partes con otro servidor de mismas características Escalamiento con el administrador del centro de cómputo.

Nombre del Servicio:	***Switch Core Redes de datos***
Objetivo:	Proporcionar de forma eficiente una interconexión completa entre los switch de pisos, el switch de servidores, el firewall y los canales de internet y telefonía existentes en la entidad.
Descripción:	Dentro de la infraestructura del centro de cómputo existen elementos los cuales son de una altísima criticidad entre ellos encontramos el switch marca Hp modelo 5120 de 48 puertos. Este elemento ubicado en el centro de cómputo del piso 16 permite la operación de todos los servicios de red que presta la O.A.P.S. en este equipo se tiene configuradas las 7 vlan existentes las cuales son para los pisos, la red inalámbrica, la red de servidores, telefonía, el segmento para los switch, entre otros, de igual manera es el encargado de interconectar los switch de los pisos que son los que alimentan cada punto de red físico en cada puesto de trabajo sobre los 3 pisos de la entidad, los switch de servidores el cual es un procure donde llegan todas las conexiones de los servidores existentes, está conectado con el firewall de la entidad, los canales de internet principal y secundario.
Necesidades que satisface:	Todos los servicios de red de la superintendencia de la economía solidaria.
Responsable del Servicio:	Oficina asesora de planeación y sistemas. ext 10152
Políticas:	No se tienen establecidas políticas sobre este elemento.
Seguridad:	1. Seguridad perimetral de control acceso al centro de computo 2. Equipo con password de administrador. 3. Deshabilitado para manipulación mediante web, se debe realizar de forma local. 4. Se le realizo backup sobre la configuración de este dispositivo, la tiene la coordinación de la oficina en medio externo.
Características de la falla:	1. Daño físico sobre el switch 2. Des-configuración del switch 3. Modificación sobre las conexiones existentes, esto obedeciendo a las diferentes configuraciones sobre los puertos de este equipo.

Impacto:	1
Código de prioridad:	1
Resolución y Recuperación:	Reconfiguración de equipo. Cambio de equipo con uno de los switch destinados para pisos. Escalamiento con el administrador del centro de cómputo.

Nombre del Servicio:	***Sistema de Gestión Documental de Archivos Electrónicos eSigna***
Objetivo:	Proporcionar de forma eficaz un servicio para la gestión de la correspondencia oficial de la Superintendencia de la Economía Solidaria.
Descripción:	Permite desarrollar el registro de la correspondencia oficial que llega a la entidad a través de la digitalización de los documentos, de igual forma permite redireccionar desde el área de correspondencia al área competente para realizar la gestión correspondiente, ya sea generando nuevos expedientes, gestionando documentos de respuesta o permitiendo generar nuevos documentos para circulación interna y externa de la Superintendencia de la Economía Solidaria. A través de este servicio es posible acceder a las siguientes soluciones: Gestión de correspondencia: La gestión de correspondencia, permite la administración y control de todos los documentos oficiales que ingresan o salen de la Superintendencia de la Economía Solidaria. Gestión de correspondencia interna: Permite gestionar la correspondencia interna generada por los usuarios de la Superintendencia de la Economía Solidaria directamente en el sistema de gestión documental de archivos electrónicos eSigna. Gestión de correspondencia externa: Permite realizar la digitalización de la correspondencia externa para que los documentos sean gestionados mediante el sistema de gestión de documental de archivos electrónicos eSigna.
Necesidades que satisface:	Gestión de correspondencia de la Superintendencia de la Economía Solidaria.
Responsable del Servicio:	Oficina Asesora de Planeación y Sistemas Ext: 10132
Políticas:	Para el manejo del servicio se establecen las siguientes políticas: 1. La Oficina Asesora de Planeación y Sistemas prestará el servicio y su soporte según lo establecido en los acuerdos pactados con los usuarios sobre la solicitud del servicio.

	2. La Oficina Asesora de Planeación y sistemas debe programar capacitaciones a los usuarios sobre el uso del servicio antes de habilitar el acceso. 3. Es responsabilidad de cada usuario el manejo de sus contraseñas de acceso al servicio y se deben realizar de la siguiente manera: - La contraseña debe tener mínimo ocho (8) caracteres - La contraseña debe tener un carácter en mayúscula uno en minúscula y uno alfanumérico (ej. Cordoba2017*). - Las contraseñas son de uso personal e intransferible. 4. El usuario se hace responsable por el adecuado uso del servicio, en caso de requerir capacitación deberá solicitarla con la Oficina Asesora de Planeación y Sistemas. 5. La solicitud y soporte del servicio se realiza a través de la Mesa de servicios en la Intranet de la Superintendencia de la Economía Solidaria. En caso de ser necesario el usuario podrá realizar una nueva solicitud de capacitación enviando un ticket a través de la mesa de servicios o comunicándose a la extensión 10132 de la Oficina Asesora de Planeación y Sistemas.
Seguridad:	Existen perfiles definidos que son utilizados para la consulta de documentos en el sistema de gestión documental de archivos electrónicos eSigna, los cuales determinan el nivel de acceso y seguridad requerido para la información. Los jefes de cada área son las personas que definen que tipo de confidencialidad de asigna a los usuarios teniendo en cuenta la necesidad del área y la responsabilidad del usuario. Para la seguridad de la información, se definen diferentes permisos para la consulta en el sistema de gestión documental de archivos electrónicos eSigna de la siguiente manera: 1. Gestor: Permite al usuario realizar la consulta de sus tareas realizadas y los documentos que pertenecen a su unidad organizativa. 2. Coordinador: Permite al usuario realizar la consulta de la información que se encuentra asignada en cada uno de los gestores de su unidad organizativa. 3. Delegados Intendentes y Jefes de Oficina: Permite al usuario realizar la consulta de todos los coordinadores que hacen parte de la unidad organizativa, así como los gestores que pertenecen al mismo. 4. Superintendente: Permite al usuario realizar la consulta de toda la información de todas las unidades organizativas.

	5. Administrador: Permite al usuario realizar la consulta de toda la información registrada en cada uno de los niveles de seguridad.
Características de la Falla:	Caída del servicio del sistema de gestión documental eSigna
Impacto:	1
Código de prioridad:	1
Resolución y Recuperación:	Escalamiento con el administrador del sistema y luego los proveedores relacionados con el servicio para su respectivo restablecimiento. Ver Anexo 1

Nombre del Servicio:	***Sistema de Gestión Documental de Archivos Electrónicos eSigna***
Objetivo:	Proporcionar de forma eficaz un servicio para la gestión de la correspondencia oficial de la Superintendencia de la Economía Solidaria.
Descripción:	Permite desarrollar el registro de la correspondencia oficial que llega a la entidad a través de la digitalización de los documentos, de igual forma permite redireccionar desde el área de correspondencia al área competente para realizar la gestión correspondiente, ya sea generando nuevos expedientes, gestionando documentos de respuesta o permitiendo generar nuevos documentos para circulación interna y externa de la Superintendencia de la Economía Solidaria. A través de este servicio es posible acceder a las siguientes soluciones: Gestión de correspondencia: La gestión de correspondencia, permite la administración y control de todos los documentos oficiales que ingresan o salen de la Superintendencia de la Economía Solidaria. Gestión de correspondencia interna: Permite gestionar la correspondencia interna generada por los usuarios de la Superintendencia de la Economía Solidaria directamente en el sistema de gestión documental de archivos electrónicos eSigna. Gestión de correspondencia externa: Permite realizar la digitalización de la correspondencia externa para que los documentos sean gestionados mediante el sistema de gestión de documental de archivos electrónicos eSigna.
Necesidades que satisface:	Gestión de correspondencia de la Superintendencia de la Economía Solidaria.
Responsable del Servicio:	Oficina Asesora de Planeación y Sistemas Ext: 10132
Políticas:	Para el manejo del servicio se establecen las siguientes políticas:

	6. La Oficina Asesora de Planeación y Sistemas prestará el servicio y su soporte según lo establecido en los acuerdos pactados con los usuarios sobre la solicitud del servicio. 7. La Oficina Asesora de Planeación y sistemas debe programar capacitaciones a los usuarios sobre el uso del servicio antes de habilitar el acceso. 8. Es responsabilidad de cada usuario el manejo de sus contraseñas de acceso al servicio y se deben realizar de la siguiente manera: - La contraseña debe tener mínimo ocho (8) caracteres - La contraseña debe tener un carácter en mayúscula uno en minúscula y uno alfanumérico (ej. Cordoba2017*). - Las contraseñas son de uso personal e intransferible. 9. El usuario se hace responsable por el adecuado uso del servicio, en caso de requerir capacitación deberá solicitarla con la Oficina Asesora de Planeación y Sistemas. 10. La solicitud y soporte del servicio se realiza a través de la Mesa de servicios en la Intranet de la Superintendencia de la Economía Solidaria. En caso de ser necesario el usuario podrá realizar una nueva solicitud de capacitación enviando un ticket a través de la mesa de servicios o comunicándose a la extensión 10132 de la Oficina Asesora de Planeación y Sistemas.
Seguridad:	Existen perfiles definidos que son utilizados para la consulta de documentos en el sistema de gestión documental de archivos electrónicos eSigna, los cuales determinan el nivel de acceso y seguridad requerido para la información. Los jefes de cada área son las personas que definen que tipo de confidencialidad de asigna a los usuarios teniendo en cuenta la necesidad del área y la responsabilidad del usuario. Para la seguridad de la información, se definen diferentes permisos para la consulta en el sistema de gestión documental de archivos electrónicos eSigna de la siguiente manera: 6. Gestor: Permite al usuario realizar la consulta de sus tareas realizadas y los documentos que pertenecen a su unidad organizativa. 7. Coordinador: Permite al usuario realizar la consulta de la información que se encuentra asignada en cada uno de los gestores de su unidad organizativa. 8. Delegados Intendentes y Jefes de Oficina: Permite al usuario realizar la consulta de todos los coordinadores que hacen parte de la unidad organizativa, así como los gestores que pertenecen al mismo.

	9. Superintendente: Permite al usuario realizar la consulta de toda la información de todas las unidades organizativas. 10. Administrador: Permite al usuario realizar la consulta de toda la información registrada en cada uno de los niveles de seguridad.
Características de la Falla:	Fallas de Firma Digital.
Impacto:	2
Código de prioridad:	2
Resolución y Recuperación:	Escalamiento con el administrador del sistema y luego los proveedores relacionados con el servicio para su respectivo restablecimiento. Ver Anexo 1

Responsable del documento: **OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS**