# Servicios TI

- Gestión de Infraestructura
- Gestión de Software TI
- Demanda y Capacidad TI
- Gestión de Disponibilidad y Continuidad
- Gestión de Proveedores y Contratos
- Soporte de Servicios TI

# Gestión de Infraestructura

# 1. Red

1.1 ¿Se tienen identificados los componentes de red?

- Se deben poder identificar los componentes de la red, tales como Router, Switch, Firewall, Canales de Internet, VPN's

1.2 Se deben poder identificar los componentes de la red, tales como Router, Switch, Firewall, Canales de Internet, VPN's

- Se deben poder identificar las configuraciones de la red, tales como Router, Switch, Firewall, Canales de Internet, VPN's

1.3 ¿Se tienen identificados los usuarios de la red?

- Se debe poder saber ¿Quién está conectado?

1.4 ¿Se tiene filtrado el contenido entrante y saliente de la red?

- Firewall

# 2. Dispositivos tecnológicos

2.1 ¿La organización cuenta con un repositorio que permita identificar cada uno de sus dispositivos tecnológicos?

- CMS

2.2 ¿Se cuenta con un control de la configuración de cada dispositivo tecnológico?

- Asignación; Históricos; Prestamos; de: Computadores; Servidores; Celulares; Proyectores; Impresoras

2.3 ¿Se realiza mantenimiento preventivo sobre los dispositivos tecnológicos?

- Asignación; Históricos; Prestamos; de: Computadores; Servidores; Celulares; Proyectores; Impresoras

# 3 Activos Fisicos

3.1 ¿Se tiene un inventario de los activos fisicos de TI , incluyendo el etiquetado físico si fuera necesario?

- Armarios; Aire Acondicionados; Repuestos de hardware;

# 4. Datacenter

4.1 ¿Se cuenta con el control de acceso fisico a los Centros de Datos de TI?

4.2 ¿Se realiza un control de la temperatura del centro de datos y los dispositivos en el?

4.3 ¿Se realiza un mantenimiento físico a las instalaciones de los Centros de Datos?

4.4 ¿Se cuenta con sistemas de respaldo energético para los Centros de Datos?

4.5 ¿Se hace la Referenciación de los Dispositivos Tecnológicos de manera precisa?

# Gestión de Software TI

# 1. Arquitectura de Software

1.1 ¿Se identifican las arquitecturas de los respectivos sistemas de información?

- Diseño fundamental que incluye los diferentes componentes y atributos (Funcionalidad, usabilidad, tolerancia a cambios, performance, reutilización, aspectos estéticos ) y la forma en que interactuan entre sí y las relaciones entre ellos.

1.2 ¿Se identifican los sistemas de información críticos para la organización?

- Hace referencia a aquellas aplicaciones que bajo ninguna circunstancia se pueden manipular o tocar porque por ejmplo no se cuenta con el soporte adecuado, están desarrolladas en un leguaje poco conocido, hay pocos o no existe soporte en el mercado, etc

# 2. Control de Software TI

2.1 ¿La organización cuenta con catálogo actualizado de los sistemas de información y sus respectivos atributos?

- Directorio actualizado de los sistemas de información, que incluya los atributos relevantes (nombre del sistema, descripción del sistema, estado (Desarrollo, Pruebas, Producción), plataforma de aplicaciones, plataforma de base de datos, proveedor, descripción del servicio, lenguaje de programación, categoría (Misional, de apoyo, financiero, administrativo, portales, transversal) y la relaciones entre ellos.

2.2 ¿Se tiene control sobre el licenciamiento de los dispositivos tecnológicos de TI?

# 3. interfaces

3.1 ¿Se identifican las interfaces entre los sistemas de información?

- Cualquier sistema de información en algún momento necesita comunicarse con otro, por lo que se hace necesario definir las fronteras, límites para esta comunicación. Ejemplo: El sistema de gestión de accesos del personal está comunicado con el sistema de nómina, esto con el fin de reportar los retrasos, incumplimientos en los horarios de llegada y así poder efectuar los descuentos correspondientes.

# 4. Control de Configuración

4.1 ¿Para cada uno de los sistemas de información se cuenta con la documentación técnica?

- Documentación de usuario, técnica y de operación debidamente actualizada, que asegure la transferencia de conocimiento a los usuarios, hacia la dirección de Tecnología y hacia los servicios de soporte tecnológico

4.2 ¿Para cada uno de los sistemas de información se cuenta con la documentación de usuario final?

4.3 ¿Existe un repositorio de códigos fuente u otros activos generados para los sistemas de información?

- Por ejemplo el SVN (Apache Subversión; Bitbucket; Github; etc), herramienta de control de versiones open source.

4.4 Se tiene un sistema de gestión documental (SKMS) donde se recopile la documentación relacionada con los sistemas de información?

- Repositorio de información como Nuxeo; Alfresco; OpenKM

4.5 ¿Se tiene un control de las diferentes versiones de los sistemas de información?

# Demanda y Capacidad TI

# 1. Demanda

1.1 ¿Se recolectan y analizan métricas sobre la demanda de los servicios de acuerdo a los usuarios que utilizan dichos servicios?

- Tener en cuenta métricas como número de transacciones, recurrencia de usuarios, recursos necesarios para cubrir dicha demanda de usuarios. ¿Dónde se almacenan dichas métricas?, ¿Quién analiza las métricas?, ¿Cada cuánto se recolectan y analizan?. Verificar herramienta o documentación

1.2 ¿El personal de tecnología conoce cuáles son los servicios principales del negocio y periodos críticos en que hay mayor demanda de usuarios (Rendimiento del servicio)?

- Indagar sobre cómo se le da a conocer esta información al personal de la operación (reunión, comunicado, correo, etc)

1.3 ¿Se cuenta con identificación de los perfiles de los usuarios a partir de las métricas y tendencias de utilización de los servicios tecnológicos?

- Revisar si existe documentación sobre la caracterización de perfiles de los usuarios internos y externos. Indagar si el personal de la operación conoce dichos perfiles de usuario

# 2. Capacidad

2.1 ¿Se realiza monitoreo a la capacidad de los servicios tecnológicos de acuerdo a su criticidad para el negocio?

- Tener en cuenta los servicios identificados en el numeral 2,2 (servicios principales del negocio). Indagar sobre herramienta o software utilizado para el monitoreo y cada cuanto se revisa la información

2.2 ¿De acuerdo al monitoreo de los servicios tecnológicos (demanda y capacidad), se planifican los recursos necesarios para responder adecuadamente a los cambios en la demanda de los servicios tecnológicos (plan de capacidad)?

- Tener en cuenta los resultados del monitoreo de la demanda y de la capacidad de los servicios tecnológicos. ¿qué sucede cuando se identifican periodos pico de utilización de los servicios?, ¿se planifica la respuesta a la demanda de usuarios?, ¿Quién tiene la autoridad para facilitar los recursos o infraestructura requerida?

2.3 ¿Se realiza la supervision de la capacidad planificada frente a la capacidad utilizada?

- se recomienda utilizar algún tipo de software que permita supervisar el comportamiento del plan de capacidad, ¿Quién realiza la supervisión?

2.4 ¿Frecuentemente se toman decisiones o acciones correctivas sobre la capacidad de los servicios tecnológicos teniendo como base los resultados de la supervisión de la capacidad?

- ¿Quién toma las decisiones?, ¿se deja evidencia de la toma de decisiones o sobre los cambios hechos al plan de capacidad?, ¿Cada cuánto se realizan revisiones al plan de capacidad?

2.5 ¿Se conoce la capacidad de los servicios?

¿Se conoce la capacidad de los servicios?

2.6 ¿Están determinados los criterios de desempeño y capacidad como funciones vitales del negocio, retrasos aceptables, degradación del rendimiento aceptable (factor de escala)?

- Validar con los SLM

# Gestión de Disponibilidad y Continuidad

# 1. Disponibilidad

1.1 ¿Se monitorean los eventos generados por los activos y/o servicios tecnológicos?

- Tener en cuenta los servicios principales, o servicios críticos para la operación del negocio; Preferiblemente contar con una herramienta o software que permita tal monitoreo

1.2 ¿Se cuenta con un plan de Alta disponibilidad para los servicios tecnológicos que se ajuste a los objetivos y prioridades del negocio?

- ¿La operación conoce el plan de alta disponibilidad?, ¿La operación conoce cuáles son los objetivos y prioridades del negocio?. Si no existe un plan formal, ¿cómo responde la operación frente a la caída de un servicio?: ¿se cuenta con un canal de respaldo?, ¿se realiza backup a los servidores?, ¿Los servidores de respaldo suben automáticamente?

1.3 ¿Frecuentemente se realizan pruebas de los planes de Alta disponibilidad como medida proactiva frente a fallas críticas de los servicios tecnológicos?

- ¿Cada cuánto se realizan las pruebas del plan de disponibilidad?, ¿Se planifican las pruebas?, ¿Quién las hace?, ¿Qué documentación se deja como evidencia de las pruebas del plan de disponibilidad?

1.4 ¿El personal de tecnología tiene conocimiento del plan de Alta disponibilidad y cómo ponerlo en marcha cuando es requerido?

- Revisar si existe un procedimiento documentado, contacto con proveedores,

1.5 ¿Se realiza la supervisión de los planes de Alta disponibilidad teniendo en cuenta los objetivos y prioridades del negocio?

- Verificar la existencia de evidencia sobre alguna reunión o revisión de los planes de alta disponibilidad, en la que se demuestre que la alta gerencia está involucrada. Tener en cuenta la alineación con lo que espera el negocio de acuerdo a la estrategia

1.6 ¿Frecuentemente se toman decisiones o acciones correctivas sobre los planes de Alta disponibilidad de los servicios tecnológicos teniendo como base los resultados del monitoreo de la disponibilidad?

- Tomando como base el monitoreo de la disponibilidad y el plan de disponibilidad, ¿Hay evidencia de las decisiones tomadas?, ¿Se siguen procedimientos para la toma de decisiones?¿Se cuenta con un plan de mejoras a la disponibilidad?

1.7 ¿Existe recopilación de datos necesarios para medir la disponibilidad?

- ¿Se cuenta con indicadores?¿Se realiza seguimiento, análisis y reporte de la disponibilidad de sus servicios y/o componentes?

# 2. Continuidad

2.1 ¿Se identifican y gestionan los incidentes que generan la NO continuidad de los servicios tecnológicos?

- Tener en cuenta la herramienta de gestión de incidentes para filtrar los incidentes relacionados con la falta de continuidad de los servicios tecnológicos
- Se debería asegurar la disponibilidad y rendimiento de los servicios en niveles suficientes en caso de desastre
- Se gestionan las dependencias de los servicios y se mantienen bajo medidas de control para prevenir la caída de los servicios

2.2 ¿Existe un procedimiento estandarizado para la ejecución, almacenamiento y prueba de las copias de seguridad (backups)?

- Indagar sobre el procedimiento establecido para la ejecución de backups. ¿El personal de la operación conoce y maneja claramente el procedimiento? Indicar qué incluye el procedimiento

2.3 Cuenta la organización con planes de contingencia y continuidad de negocio?

- Plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada

# 3. Riesgos

3.1 ¿Existen lineamientos ó guías claras para la gestión de riesgos de T.I?

- Indagar sobre la documentación existente sobre cómo funciona la gestión de riesgos de T.I., políticas, partes involucradas, información requerida, herramienta o software autorizado, métricas, cultura de gestión de riesgos, frecuencia de las actividades de gestión de riesgo. Verificar si estas guías cumplen un ciclo de identificación, análisis, evaluación, controles (tratamientos), monitoreo y revisión

3.2 ¿Se gestionan los riesgos asociados a los servicios tecnológicos?

- Verificar si existe evidencia de la gestión de riesgos del área de T.I. (evidencia sobre algun tipo de software o herramienta). Quién hace la identificación de riesgos, cómo lo hace, cada cuanto lo hace, como se analizan los riesgos, categorías de riesgo, respuesta a los riesgos, controles. Tener en cuenta los servicios tecnológicos principales o críticos para la operación del negocio. Verificar si existe evidencia sobre algun software o herramienta. Se debe encontrar principalmente información técnica de cada servicio, la gestión de riesgos debe tener un enfoque operacional y estratégico

# Gestión de Proveedores y Contratos

# 1. Gestión de la Información de Proveedores

1.1 ¿Se tienen identificados todos los proveedores que soportan las operaciones de TI según categorías?

- Algunas categorías son: Capacitación; Servicios de Red; Mantenimiento; Consultoría; Software; Infraestructura;

1.2 ¿Se tiene registro y seguimiento sobre los servicios prestados por los proveedores?

- Contratos o documentación relacionada con: Equipo y roles del equipo contratista, responsabilidades del contratista, disponibilidad del servicio y horarios de prestación del mismo, indicadores y niveles de calidad, procedimiento para transferencia de conocimiento a la entidad o a otro contratista

1.3 ¿Se tienen clasificados los proveedores según su estado?

- Inscrito; Autorizado; Suspendido; Prohibido; En Evaluación; etc

# 2. Gestión de Contratos

2.1 ¿Se definen criterios de aceptación y ANS cuando con los proveedores de Servicios TI?

- Definición de indicadores para evaluar el desempeño del servicio y el cumplimiento pactado con el contratista. Pueden incluir penalizaciones económicas si se diera a lugar.

2.2 ¿Los contratos con los proveedores poseen clausulas que permitan garantizar el cumplimiento de los mismos?

- Transferencia de derechos de autor; Penalizaciones por incumplimiento; Pólizas

2.3 ¿Se realiza una evaluación sobre la prestación de servicios de los proveedores?

- Cuando un proveedor presta servicios, debe ser evaluado a intervalos regulares para garantizar que cumple con lo acordado; Por lo general se califican númericamente (1 a 5); En algunos casos, se pueden identificar proveedores prohibidos dada su baja calificación

2.4 ¿Existe un rol especializado que realice la supervisión/seguimiento de cada contrato suscrito con los proveedores?

- Normalmente llamad@ Interventor@/Supervisor@

# Soporte de Servicios TI

# 1. Mesa de Servicio

1.1 ¿Cuenta con herramientas parametrizadas y automatizadas para brindar un soporte mas eficiente (por ejem. Chatbots, que soportan los canales tradicionales de reporte de servicios?)

1.2 ¿Se monitorea el cumplimiento de los Acuerdos de Nivel de Servicio?

1.3 ¿Los analistas o asesores de de la mesa de servicio cuentan con las heramieta adecudas para brnidar apoyo y soporte en la resolución de incidentes y solicitudes?

1.4 ¿Se tienen definidos criterios para identificar/separar los incidentes, las solicitudes y/o los problemas?

1.5 ¿Existen criterios para realizar la priorización de incidentes, solicitudes y/o problemas?

1.6 ¿Existen criterios para realizar la asignación de un Acuerdo de Nivel de Servicio a los incidentes, solicitudes y/o solicitudes?

1.7 ¿Todos los incidentes y/o solicitudes son asignados a una persona/grupo de resolución? ¿Existen criterios para realizar dicha asignación?

- Existen criterios para asignan los incidentes/solicitudes a grupos especializados cuando no se puedan resolver en el grupo de primer nivel.

# 2. Gestión de Incidentes y Solicitudes

2.1 ¿Los incidentes/solicitudes tienen relacionado el servicio afectado/involucrado?

2.2 ¿Los incidentes/solicitudes tienen relacionados los elementos de configuración afectados/involucrados?

2.3 ¿Se realiza la medición de la satisfacción de los clientes respecto a la atención/resolución de sus incidentes/solicitudes?

2.4 ¿Se usan los datos históricos y/o tendencias para prevenir la ocurrencia de incidentes?

2.5 ¿Se usan los datos históricos y/o tendencias para crear elementos de Auto-Ayuda que disminuyan la cantidad de solicitudes generadas por los usuarios?

# 3. Gestión de Problenas

3.1 ¿Se cuenta con un equipo multidisciplinar para el análisis e impacto de aquellos incidentes que pueden derivar en afectaciones más graves del servicio?

- ¿El análisis de problemas utiliza información sobre la arquitectura y la configuración del producto para identificar los elementos de configuración (CI) que probablemente causen los incidentes relevantes?

3.2 ¿Los problemos identificados, actualmente cuentan con un analisis de causa raíz ?

3.3 ¿Se cuenta con un control efectivo de los errores conocidos, es decir, se cuenta con información actualizada sobre todos los errores conocidos de sus productos, incluidos sus estados, y el impacto de estos en los servicios?

# 4. Investigación y resolución de los incidentes

4.1 ¿Se notifica formalmente a las partes interesadas sobre el estado de sus incidentes/solicitudes?

4.2 Cuando para la resolución del incidente/solicitud se requiere realizar un cambio, se realiza siguiendo un proceso/control de cambios

4.3 ¿Se mide el tiempo que tarda el incidente/solicitud en un área/equipo?

4.4 Cuando se cierra el incidente/solicitud, se detalla la solución aplicada? ¿Existen categorías para esta información?

- Confirmar con el usuario/grupo afectado que la solución aplicada a su incidentes/solicitud fue satisfactoria (antes de realizar el cierre en la herramienta)

4.5 Existe y se mantiene actualizada una Base de Conocimiento

- Registrar si se usaron soluciones temporales para resolver los incidentes