ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

AUDITORÍA DEL SISTEMA INFORMÁTICO DEL MINISTERIO DE TRANSPORTE Y OBRAS PÚBLICAS

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

AUTOR:

MARÍA BELÉN MOREIRA CASTRO

mabe_mrr@hotmail.es

Director: MSc. Ing. César Gustavo Samaniego Burbano

gustavo.samaniego@epn.edu.ec

2015

DECLARACIÓN

Yo, María Belén Moreira Castro declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

María Belén Moreira Castro

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por María Belén Moreira Castro, bajo mi supervisión.

Ing. César Gustavo Samaniego Burbano
DIRECTOR

AGRADECIMIENTOS

Primero a Dios que me ha permitido llegar aquí y me ha dado todo.

A mis padres, mi hermana y mi sobrino por su apoyo incondicional en todo momento de mi vida, son importar la situación, sin importar el reto, siempre me han ayudado a cumplir mis metas y me han dado todo para seguir adelante.

A Ricardo, por su apoyo, comprensión y motivación, no sólo para culminar mi tesis sino en este momento de mi vida. Ha sido una luz en mi camino.

A mis abuelitas, tíos y familiares, por su ejemplo y su apoyo, en cada paso que damos en la vida llevamos a la familia. Supieron formar dos personas fantásticas que a su vez lo hacen conmigo.

A mis amigos, por estar conmigo en los buenos y sobretodo en los malos momentos, me han acompañado en lo largo del camino y han dejado huella.

A mis profesores, por sus enseñanzas, sobre todo al Ing. Gustavo Samaniego, que me ha ayudado y guiado en este camino.

Este logro no es sólo mío, es también suyo.

DEDICATORIA

A Dios.

A mis padres, todo lo que he alcanzado en mi vida es por ustedes, la persona que soy es gracias a ustedes.

A mi hermana, ahora es mi turno, espero con ansia el tuyo.

A mi sobrino, espero q mis logros te enorgullezcan y que cuando tu alcances los tuyos pueda estar siempre a tu lado.

A mi tío Raúl, siempre preocupado por los demás, yo sé que desde el cielo nos cuida.

Caminante, son tus huellas
el camino y nada más;
Caminante, no hay camino,
se hace camino al andar.
Al andar se hace el camino,
y al volver la vista atrás
se ve la senda que nunca
se ha de volver a pisar.
Caminante no hay camino
sino estelas en la mar.
- Antonio Machado

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

El presente proyecto de titulación detalla los pasos realizados en la auditoría realizada al sistema informático del Ministerio de Transporte y Obras Públicas utilizando el marco de trabajo COBIT 5.

En el Capítulo I se describe el Ministerio, y se caracteriza la Unidad Informática. Además se plantea la metodología en base al marco de trabajo COBIT 5, utilizando el modelo de capacidad y la herramienta Self-Assessment-Templates para COBIT 5.

En el Capítulo II se hace una selección de los procesos que se utilizan para la auditoría, y se realiza la auditoría tomando en cuenta los niveles de capacidad de los procesos evaluados.

En el Capítulo III se hace un análisis de los resultados obtenidos y se generan los informes. El primer informe que se genera es el informe preliminar, donde se exponen los niveles de capacidad obtenidos por cada proceso. Los otros dos informes son el informe técnico y el informe ejecutivo, los mismos que contienen las conclusiones y recomendaciones de cada proceso evaluado.

En el Capítulo IV se establecen las conclusiones y recomendaciones referentes a este proyecto de titulación.

CAPÍTULO I: DESCRIPCIÓN DEL PROBLEMA

1.1 CARACTERIZACIÓN DEL MINISTERIO

1.1.1 DESCRIPCIÓN DEL MINISTERIO

El Ministerio de Transporte y Obras Públicas (MTOP) es una empresa pública que se encarga de planificar, gestionar el desarrollo y realizar revisiones de obras de transporte e infraestructura, para impulsar el desarrollo del país. Además, debe establecer y aplicar políticas de Transporte y Obras Públicas, sobre todo para asegurar los niveles de seguridad y garantizar la satisfacción de los ciudadanos con respecto al sistema de transporte nacional y a las obras realizadas.

En la Figura 1 se encuentra el logo del MTOP y a continuación se detalla información relevante del ministerio.

Figura 1 – Logo del Ministerio de Transporte y Obras Públicas[1]

Nombre: Ministerio de Transporte y Obras Públicas (MTOP)
Ubicación: Juan León Mera N26-220 y Av. Orellana. Quito - Ecuador
Teléfono: 593-2 397-4600
Sitio Web: www.obraspublicas.gob.ec

1.1.2 MISIÓN

"Como entidad rectora del Sistema Nacional del Transporte Multimodal formula, implementa y evalúa políticas, regulaciones, planes, programas y proyectos que garantizan una red de Transporte seguro y competitivo, minimizando el impacto ambiental y contribuyendo al desarrollo social y económico del País."[2]

[1] Imagen tomada de la página web del Ministerio de Transporte y Obras Públicas www.obraspublicas.gob.ec
[2] Información tomada de la página web del Ministerio de Transporte y Obras Públicas http://www.obraspublicas.gob.ec/el-ministerio/

1.1.3 VISIÓN

"Ser el eje del desarrollo nacional y regional mediante la Gestión del Transporte Intermodal y Multimodal y su Infraestructura con estándares de eficiencia y Calidad."[3]

1.1.4 VALORES

El Ministerio de Transporte y Obras Públicas pone en práctica una serie de valores con el objetivo de dar un excelente servicio al país. Entre los valores más importantes se mencionan los siguientes:

- Apertura
- Calidad
- Eficiencia
- Eficacia
- Honestidad
- Lealtad
- Mejora Continua
- Responsabilidad

1.1.5 OBJETIVO

"Contribuir al desarrollo del País a través de la formulación de políticas, regulaciones, planes, programas y proyectos, que garanticen un Sistema Nacional del Transporte Intermodal y Multimodal, sustentado en una red de Transporte con estándares internacionales de calidad, alineados con las directrices económicas, sociales, medioambientales y el plan nacional de desarrollo."[4]

[3] Información tomada de la página web del Ministerio de Transporte y Obras Públicas http://www.obraspublicas.gob.ec/el-ministerio/
[4] Información tomada de la página web del Ministerio de Transporte y Obras Públicas http://www.obraspublicas.gob.ec/el-ministerio/

1.1.6 ESTRUCTURA ORGÁNICA DEL MINISTERIO

1.1.6.1 Estructura Orgánica actual del Ministerio

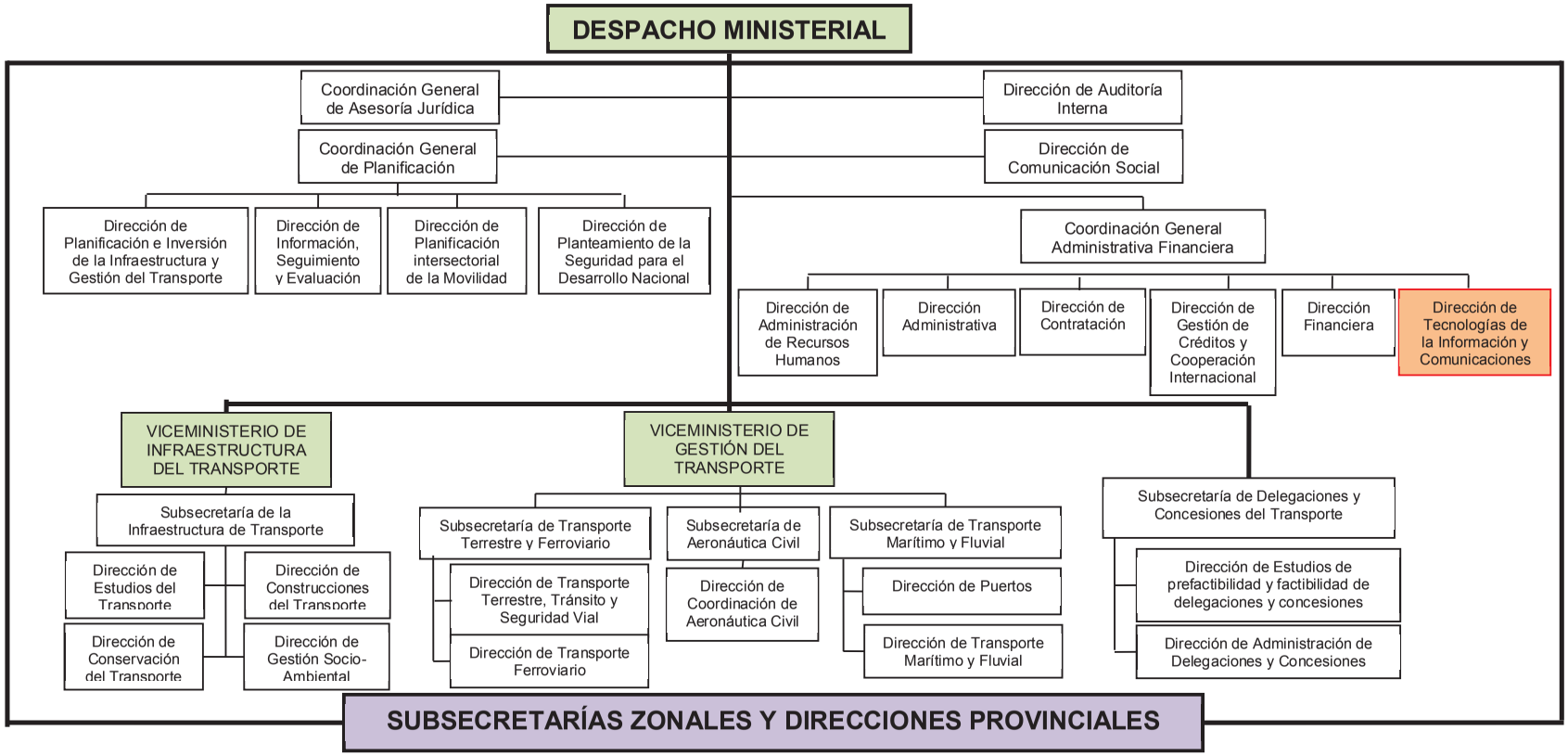


Figura 2 – Orgánico Funcional Actual del Ministerio de Transporte y Obras Públicas[5]

[5] Imagen tomada de la página web del Ministerio de Transporte y Obras Públicas www.obraspublicas.gob.ec

1.1.6.2 Estructura Orgánica aprobada por el Ministerio

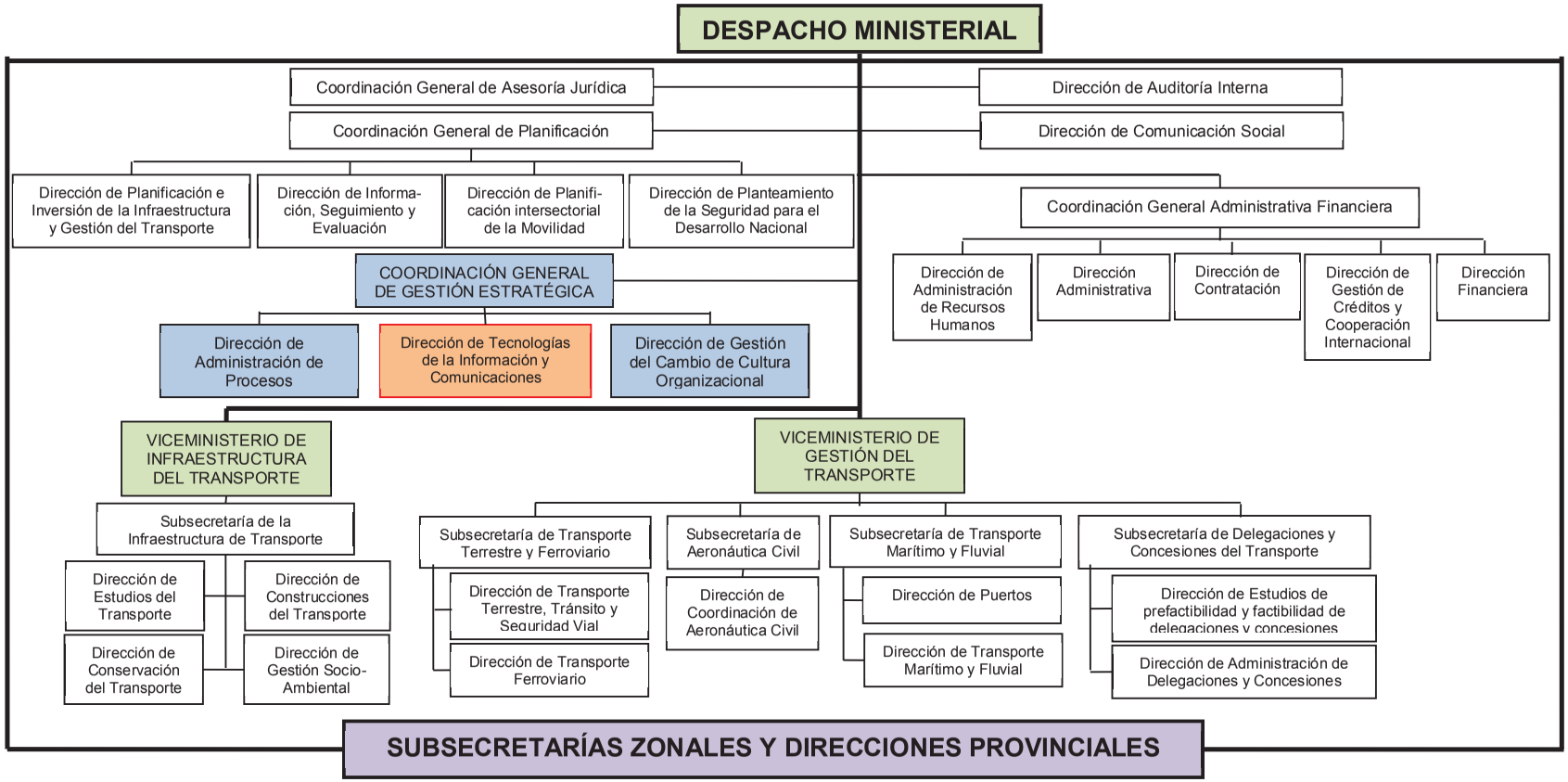


Figura 3 – Orgánico Funcional aprobada por el Ministerio de Transporte y Obras Públicas[6]

[6] Imagen tomada del Acuerdo 004 de la Coordinación General de la Planificación Estratégica. Quito, 2013

La figura 2 corresponde al Orgánico Funcional actual del MTOP y la figura 3 corresponde al Orgánico Funcional aprobado el 10 de enero del 2013 que debe ser instaurado. En el Orgánico Funcional actual la Unidad Informática llamada Dirección de la Tecnologías de la Información y Comunicación se halla ubicada debajo de la Coordinación General de la Administración Financiera. Según las mejores prácticas el nivel que la Unidad Informática debe ocupar es un nivel de Dirección de asesoría informática al Ministro, debe estar presente en la toma de decisiones, no como una herramienta de apoyo sino como un elemento fundamental, tal y como lo requieren las necesidades de la sociedad actual.
El Orgánico Funcional Aprobado el año 2013 ubica a la Unidad de Informática en una posición mejor referente a la que tiene en la actualidad, bajo la Coordinación General de Gestión Estratégica, pero aun así no es el nivel de decisión ideal.

1.2 CARACTERIZACIÓN DE LA UNIDAD INFORMÁTICA

1.2.1 DESCRIPCIÓN DE LA UNIDAD INFORMÁTICA

La Unidad Informática se encarga de realizar actividades relacionadas con el software, hardware y comunicaciones, tales como:

- Identificación de necesidades.
- Elaboración de informes técnicos para la adquisición.
- Capacitación tecnológica a cada persona que forma parte del Recurso Humano del MTOP, conjuntamente con la Dirección de Administración de Recursos Humanos.
- Monitoreo para asegurar su correcto funcionamiento.
- Mantenimiento, reparación y soluciones.
- Aprobar inventarios.
- Proponer el Plan de Inversiones en la Unidad.

1.2.1.1 Misión

"Administrar y proveer servicios informáticos y tecnologías de la información y comunicaciones para el procesamiento de datos y acceso a la información, garantizando la disponibilidad, seriedad, integridad y confiabilidad de la información."[7]

1.2.1.2 Ubicación

Ministerio de Transporte y Obras Públicas. 8vo piso
Juan León Mera N26-220 y Av. Orellana. Quito - Ecuador

1.2.2 ESTRUCTURA DE LA UNIDAD INFORMÁTICA

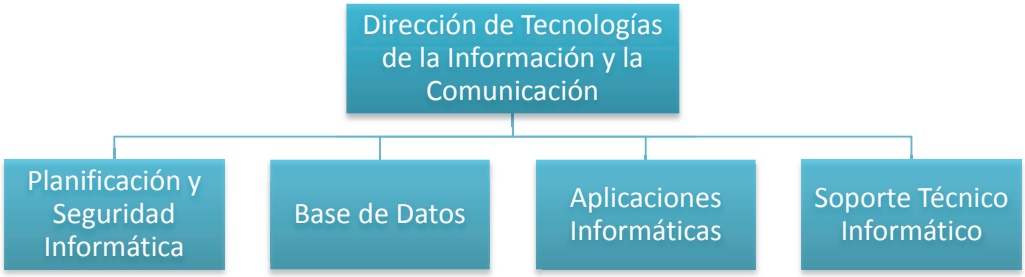


Figura 4 – Estructura Orgánica Interna de la Unidad Informática[8]

Tal como se muestra en la Figura 4 - Estructura Orgánica Interna de la Unidad Informática, la Unidad Informática en la actualidad se encuentra dividida en 4 áreas:

- Planificación y Seguridad Informática
- Bases de Datos
- Aplicaciones Informáticas
- Soporte Técnico Informático

[7] Información tomada del Estatuto Orgánico de Gestión Organizacional por procesos. Quito,
[8] Gráfico realizado por el autor

Según se establece en el Acuerdo 004 - Coordinación General Estratégica, la Dirección de Tecnologías de la Información y la Comunicación pasará a dividirse en 6 áreas:

- Planeación Estratégica, Operativa y Administración de Proyectos de TI
- Desarrollo de Sistemas Informáticos
- Infraestructura y Operaciones
- Seguridad de la Información
- Soporte Técnico
- Interoperabilidad

1.2.3 ÁREAS Y FUNCIONES

1.2.3.1 Planificación y Seguridad Informática

El área de Planificación y Seguridad Informática se encarga de establecer planes, informes y procedimientos de la Unidad Informática. Esta área se subdivide en Planificación y en Seguridad Informática. Para un mayor detalle ver Anexo 1

Los principales productos y servicios de Planificación son:

- Plan Operativo Anual y sus respectivos informes semestrales.
- Plan de Capacitación Informática e informes de evaluación trimestral.
- Informes de gestión de aplicaciones y sistemas informáticos.
- Proyecto de adquisición de software.
- Informes de soporte y capacitación.

Los principales productos y servicios de Seguridad Informática son:

- Informes de seguridad y confidencialidad de usuarios y contraseñas
- Informes de monitoreo y violaciones de seguridad
- Informes de prueba y revisiones de software
- Test de penetración al sistema operativo, redes y comunicaciones.
- Informes de Antivirus

1.2.3.2 Base de Datos

El área de Base de Datos se encarga de las operaciones que se realizan sobre las bases de datos tales como extracción, inserción, actualización y consulta de los datos.

Los principales productos y servicios son:

- Informe de cambio de información en la base y consultas.
- Informe de implementación de herramientas de optimización.
- Informe de implementación de controles y monitoreo sobre la base.
- Informes de respaldos y auditorías

1.2.3.3 Aplicaciones Informáticas

El área de Aplicaciones Informáticas se encarga de realizar actividades respecto al desarrollo de sistemas de información para el MTOP.

Los principales productos y servicios son:

- Plan Estratégico de la Unidad y Plan de Mantenimiento de Sistemas de Información
- Informes de actividades y proyectos de desarrollo de sistemas de información y su ejecución.
- Informe de mantenimiento, evaluación y monitoreo de sistemas de información.
- Informes de asesoría que involucre el desarrollo de sistemas informáticos.
- Propuestas de mejoras e innovaciones en los procesos, procedimientos y normatividad en la Unidad.

1.2.3.4 Soporte Técnico Informático

El área de Soporte Técnico Informático se subdivide en dos: Mantenimiento, y Redes y Telecomunicaciones.

Los principales productos y servicios de Mantenimiento son:

- Inventario de hardware.

- Informes de mantenimiento de equipos informáticos y actualizaciones de sistemas operativos.
- Informes de gestión de: licencias comerciales, correo electrónico, activos informáticos, servicio de Internet.
- Informes de aplicación de políticas de seguridad informática.
- Informes de actualización de antivirus y estadísticas de malware.

Los principales productos y servicios de Redes y Telecomunicaciones son:

- Informes sobre proyectos de infraestructura tecnológica.
- Informes de administración de: red telefónica, red de datos, interconexión de locales.
- Informes de la aplicación de políticas de seguridad en redes.
- Informes de monitoreo de tráfico en canales de comunicación.
- Propuestas de aplicación de tecnologías de comunicación a los procesos, como resultados de proyectos de investigación.

1.2.4 PLANES DE LA UNIDAD INFORMÁTICA

Los planes con los que cuenta la Unidad Informática son:

PLANES	Sí	Parcial	No
Plan de Implementación y desarrollo de sistemas informáticos			X
Plan de Capacitación			X
Plan de Contingencia			X
Plan de Contratación			X
Plan de Control y Mantenimiento de Normas			X
Plan Estratégico			X
Plan Operativo			X
Plan de respaldos			X

Tabla 1- Planes de la Unidad Informática del MTOP[9]

Tal como se muestra en la Tabla 1- Planes de la Unidad Informática del MTOP, no se cuenta con ningún plan implementado o en desarrollo.

[9] Fuente: Autora

1.2.5 SISTEMA INFORMÁTICO

El sistema Informático se considera:

- Recurso Humano: El sistema informático está conformado por 25 personas.
- Software:
    - Sistema Operativo Usuarios: Windows XP, Windows 7 y Windows 8
    - Sistema Operativo: Servidores: Linux
    - Soluciones Ofimáticas: Microsoft Office, Free Office
    - Otros: Navegadores de Internet, Adobe Reader, Winrar, entre otros.
- Hardware:
    - Pc´s de Escritorio: 433
    - Laptops: 77
    - Servidores: 28
    - Impresoras: 57
    - Teléfonos IP: 500
    - Access Point: 30
    - Entre otros.
- Información: Se refiere a toda la información que se maneja en la Unidad Informática.

1.3 MÉTODO DE LA AUDITORÍA

El método con el que se desarrolló la Auditoría se basa en la Norma 410, Tecnología de la Información, del Acuerdo 039 de las Normas de Control Interno emitidos por la Contraloría General, aplicando el marco de trabajo de COBIT 5. La norma completa se encuentra en el Anexo 2, sin embargo en la sección 2.1.1 Normas de Control Interno para el MTOP se la resume y posteriormente se seleccionan los procesos de COBIT que serán evaluados.
COBIT es el acrónimo para Control Objectives for Information and related Technology, o en español Objetivos de Control para la Información y Tecnologías relacionadas.

COBIT 5 es un modelo creado por ISACA que se adapta a las necesidades de las empresas sin importar su tamaño o naturaleza, ya sea privada o pública.

Para la presente Auditoría se va a trabajar con los procesos de COBIT y el Modelo de Capacidad, para ello lo primero que se requiere es seleccionar los procesos con los que se va a trabajar. COBIT 5 tiene 37 procesos que se agrupan en 5 dominios. El primer dominio: EDM (Evaluar, Dirigir y Monitorear), pertenece al Gobierno de TI. El Gobierno de TI asegura que se evalúan las necesidades de las partes interesadas y establece las acciones necesarias para cumplir con los objetivos empresariales teniendo en cuenta la priorización y toma de decisiones.
Los otros 4 dominios: APO (Alinear, Planear y Organizar), BAI (Construir, Adquirir e Implementar), DSS (Entregar, dar Servicio y Soporte) y MEA (Monitorear, Evaluar y Valorar) son dominios de gestión. La gestión se encarga de planificar, construir, ejecutar y monitorear las actividades establecidas por el gobierno para cumplir con los objetivos de la organización.

1. Evaluar, Dirigir y Monitorear (EDM)
    - (EDM01) Asegurar que se fija el Marco de Gobierno
    - (EDM02) Asegurar la Entrega de Valor
    - (EDM03) Asegurar la Optimización de los Riesgos
    - (EDM04) Asegurar la Optimización de los Recursos

- (EDM05) Asegurar la Transparencia a las partes interesadas

2. Alinear, Planear y Organizar(APO)
    - (APO01) Administrar el Marco de la Administración de TI
    - (APO02) Administrar la Estrategia
    - (APO03) Administrar al Arquitectura Corporativa
    - (APO04) Administrar la Innovación
    - (APO05) Administrar el Portafolio
    - (APO06) Administrar el Presupuesto y los Costos
    - (APO07) Administrar el Recurso Humano
    - (APO08) Administrar las Relaciones
    - (APO09) Administrar los Contratos de Servicio
    - (AP010) Administrar los Proveedores
    - (AP011) Administrar la Calidad
    - (AP012) Administrar los Riesgos
    - (AP013) Administrar la Seguridad
3. Construir, Adquirir e Implementar(BAI)
    - (BAI01) Administrar Programas y Proyectos
    - (BAI02) Administrar la definición de Requerimientos
    - (BAI03) Administrar la Identificación y Construcción de Soluciones
    - (BAI04) Administrar la Disponibilidad y Capacidad
    - (BAI05) Administrar la Habilitación del Cambio
    - (BAI06) Administrar Cambios
    - (BAI07) Administrar la Aceptación de Cambios y Transiciones
    - (BAI08) Administrar el Conocimiento
    - (BAI09) Administrar los Activos
    - (BAI10) Administrar la Configuración
4. Entregar, dar Servicio y Soporte(DSS)
    - (DSS01) Administrar las Operaciones
    - (DSS02) Administrar las Solicitudes y los servicios incidentes
    - (DSS03) Administrar Problemas
    - (DSS04) Administrar la Continuidad
    - (DSS05) Administrar los Servicios de Seguridad

- (DSS06) Administrar los Controles en los Procesos de Negocio

5. Monitorear, Evaluar y Valorar (MEA)
    - (MEA01) Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento
    - (MEA02) Monitorear, Evaluar y Valorar el Sistema de Control Interno
    - (MEA03) Monitorear, Evaluar y Valorar el Cumplimiento con los Requisitos Externos

En la figura 5 – Procesos de COBIT 5, se encuentran graficados todos los dominios y procesos:

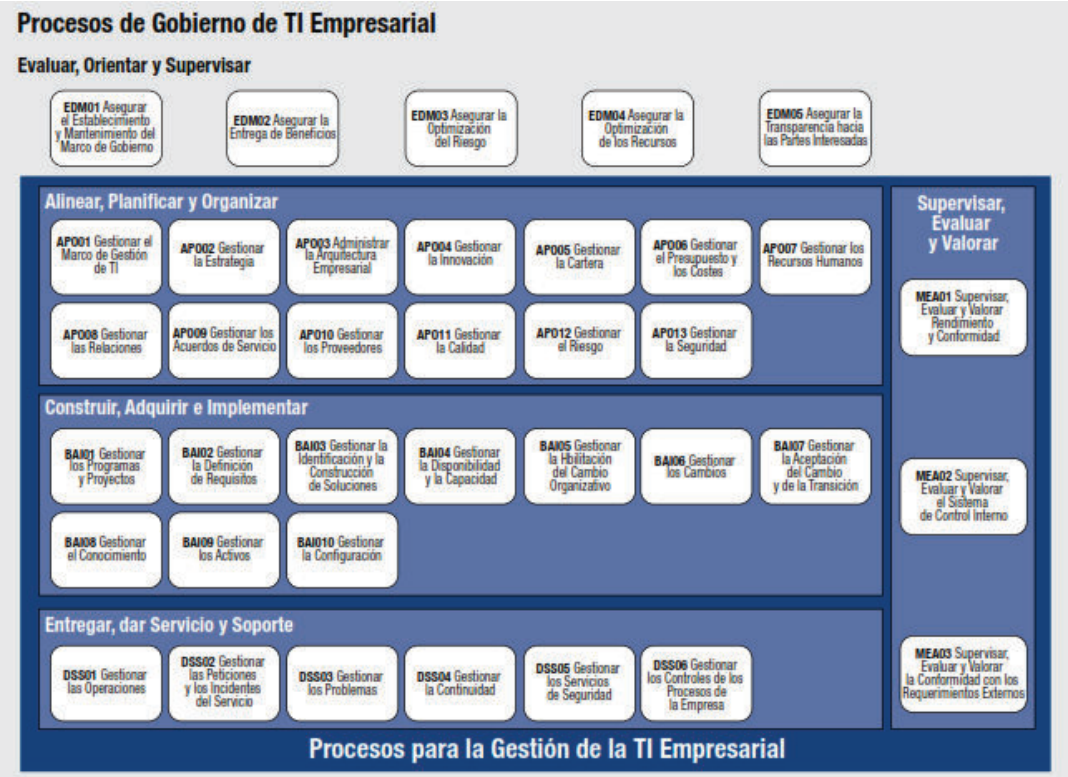


Figura 5 – Procesos de COBIT 5[10]

Una vez seleccionados los procesos, se va a utilizar la herramienta Self-Assessment-Templates para COBIT 5 para evaluar el nivel de capacidad.

Usando COBIT se va a definir el estado actual de la Unidad Informática y las actividades que deben realizarse para llegar a la situación deseada.

[10] Imagen tomada del Framework de COBIT 5, versión en Español, página 13

CAPÍTULO II: EJECUCIÓN DE LA AUDITORÍA

2.1 PLANIFICACIÓN

2.1.1 NORMAS DE CONTROL INTERNO PARA EL MTOP

La selección de los dominios y procesos de COBIT se hará tomando en cuenta las Normas de Control Interno (NCI) emitidas por la Contraloría General del Estado, Acuerdo 039, en el año 2009. Este documento es el que se encuentra vigente en la actualidad, se lo conoce como NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y PERSONAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS.

Para el presente estudio se va a utilizar la **Norma 410** referente a TECNOLOGÍA DE LA INFORMACIÓN. A continuación se describe la norma, para más información la norma completa se encuentra en el Anexo 2

410 TECNOLOGÍA DE LA INFORMACIÓN

410-01. Organización Informática:

Dentro de la norma se establece que la Unidad de Tecnologías de la Información debe:

- Trabajar en base a un marco de trabajo que asegure transparencia, control e involucre la alta dirección.
- Estar posicionada en un nivel gerencial en la estructura organizacional y no depender de otras áreas.
- Establecer revisiones periódicas de la estructura organizacional para ajustar estrategias y cumplir objetivos

410-02. Segregación de funciones:

Según la norma se establece que los roles del personal debe:

- Ser definidos claramente y formalmente comunicados, asegurándose de que exista suficiente autoridad y respaldo.
- Ser documentados teniendo en cuenta deberes, responsabilidades, habilidades y experiencia necesarios para cada posición.

410-03. Plan informático estratégico de tecnología:

Según la norma se debe:

- Elaborar un plan informático estratégico alineado con el plan estratégico institucional que contenga e incluir análisis de la situación actual y propuestas de mejora.
- Elaborar planes operativos alineados al plan estratégico y a los objetivos estratégicos.
- Aprobar los planes por la máxima autoridad de la organización e incorporarlos al plan presupuesto anual del Ministerio.
- Monitorear y evaluar los planes trimestralmente para verificar el grado de ejecución y tomar medidas en caso de ser necesario.

410-04. Políticas y procedimiento

Las políticas y procedimientos deben:

- Ser aprobados por la máxima autoridad del Ministerio.
- Permitir la asignación del personal calificado e infraestructura tecnológica necesaria.
- Ser definidos, documentados, difundidos y actualizados permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.
- Considerar los siguientes temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software.
- Incorporar directrices, estándares tecnológicos, controles, sistemas de aseguramiento de la calidad y gestión de riesgos.
- Implementar planes para monitorear y medir el cumplimiento con indicadores de desempeño.

410-05. Modelo de información organizacional

Según la norma el modelo de información organizacional debe:

- Garantizar la disponibilidad, integridad, exactitud y seguridad de la información.
- Incluir reglas de validación, controles de integridad y consistencia de los datos
- Clasificar los datos para especificar y aplicar niveles de seguridad.

410-06. Administración de proyectos tecnológicos

La unidad de tecnología de información debe:

- Documentar los proyectos tecnológicos.
- Realizar un cronograma de actividades que incluya responsables, recursos y contemple pruebas y capacitación.
- Monitorear avances del proyecto
- Incluir análisis de riesgos, control de cambios y un plan para el aseguramiento de la calidad.

410-07. Desarrollo y adquisición del software aplicativo:

La unidad de tecnología de información se encargará de:

- Documentar los proyectos de desarrollo y adquisición de Software.
- Realizar un cronograma de actividades que incluya responsables, recursos y contemple pruebas y capacitación.
- Monitorear avances del proyecto
- Incluir análisis de riesgos, control de cambios y un plan para el aseguramiento de la calidad.

410-08. Adquisiciones de infraestructura tecnológica:

La unidad de tecnologías de la información debe

- Realizar un análisis documentado de la necesidad de adquisiciones tecnológicas
- Planificar el incremento de capacidad, evaluar riesgos tecnológicos, costos, vida útil considerando los requerimientos de la carga laboral.
- Detallar los contratos sobre características técnicas de los equipos adquiridos.

410-09. Mantenimiento y control de infraestructura tecnológica

La unidad de tecnología de la Información se encarga de

- Definir procedimientos para el uso y mantenimiento adecuado de la infraestructura tecnológica.
- Definir procedimientos para mantenimiento, despliegue, corrección y mejoramiento de software y documentar los cambios.
- Controlar y registrar las versiones de software.
- Actualizar y difundir manuales técnicos y de usuario según los cambios.

- Elaborar planes de mantenimiento preventivo y correctivo, y realizar revisiones periódicas, sobre todo de las aplicaciones críticas de la organización.
- Realizar inventario de bienes informáticos detallado.

410-10. Seguridad de tecnología de la información

La unidad de tecnología de información debe establecer los siguientes mecanismos para asegurar la protección de los datos:

- Establecer una ubicación adecuada con control de acceso físico a la unidad de tecnologías de la información, tener en cuenta mecanismos de control de incendios, temperatura y humedad adecuadas, entre otros.
- Respaldar la información periódicamente.
- Respaldar la información en medios físicos adecuados en caso de actualización.
- Almacenar los respaldos con información crítica en lugares externos a la organización
- Implementar seguridades para software y hardware, establecer monitoreos de seguridad, pruebas periódicas y acciones correctivas con las vulnerabilidades encontradas.
- Establecer sitios de procesamiento alternativos
- Implementar procedimientos de seguridad para el recurso humano.

410-11. Plan de contingencias

La Unidad de tecnología de información debe:

- Definir un plan de contingencias incluyendo los escenarios de contingencia, roles y responsabilidades. El plan de contingencias debe ser confidencial, una vez aprobado debe ser difundido entre el personal responsable de su ejecución.
- Establecer un plan de continuidad del negocio. En el plan se debe incluir el uso de un centro de cómputo alterno o un data center estatal compartido.
- Establecer un plan de recuperación de desastres que contemple las actividades, antes, durante y después de un desastre.
- Mantener los planes actualizados.
- Establecer un plan de respuesta a los riesgos contemplando roles críticos para administrar los riesgos de TI.

410-12. Administración de soporte de tecnologías de la información

La unidad de tecnología de información se encargará de:

- Establecer revisiones periódicas sobre la capacidad y desempeño de los recursos tecnológicos y su proyección futura.
- Establecer medidas de prevención, detección y corrección de software malicioso.
- Crear roles y perfiles de usuarios con una identificación única y estandarizada para cada usuario que actúa con la unidad de tecnología de información, ya sea interno, externo o temporal.
- Monitorear y revisar las cuentas de usuario y privilegios asociados.
- Mantener un repositorio con la documentación de hardware y software actualizado, asegurar la integridad y disponibilidad de la información. Crear respaldos

410-13. Monitoreo y evaluación de los procesos y servicios

En el monitoreo y evaluación de procesos y servicios se debe:

- Monitorear la contribución e impacto del área en el ministerio.
- Establecer métricas e indicadores para indicar el nivel de satisfacción de clientes internos y externos

410-14. Sitio web, servicios de internet e intranet

La unidad de tecnología de información debe elaborar políticas y procedimientos documentados sobre los servicios de Internet, intranet, correo electrónico y el sitio WEB del ministerio.

410-15. Capacitación informática

La unidad de tecnología de información debe encargarse de identificar las necesidades de capacitación de todo el personal del Ministerio que usen los servicios de información, desarrollar un plan de capacitación y ejecutar la capacitación.

410-16. Comité informático

La unidad informática es la encargada de crear un comité informático teniendo en cuenta el tamaño y complejidad del ministerio.

410-17. Firmas electrónicas

La unidad informática debe incorporar el uso de firmas electrónicas de acuerdo a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento, para lo cual debe:

- Verificar la autenticidad de firmas electrónicas.
- Conservar archivos electrónicos y mensajes con firmas electrónicas y asegurarse de conservar la integridad de los daros.
- Actualizar y renovar los certificados de firma electrónica.
- Asegurar la seguridad de los certificados y dispositivos portables.
- Capacitar al recurso humano en el uso de firmas electrónicas

Una vez seleccionadas las necesidades actuales del ministerio se procede a seleccionar los procesos de COBIT relacionados, realizar el mapeo y realizar la auditoría.

2.1.2 SELECCIÓN DE LOS PROCESOS DE COBIT

Para el proceso de selección se tomaron los 17 puntos de la Norma 410 de las NCI, Acuerdo 039, y conjuntamente con el Comité Informático del MTOP se seleccionaron los procesos idóneos para la realización de la Auditoría.

Primero se hizo un análisis de la situación actual del MTOP y un análisis de la situación deseada. La situación deseada se refiere a un escenario en donde la Unidad Informática cumpla con todo lo expuesto en la norma 410 para que esté de acuerdo a la Contraloría y la normativa Ecuatoriana.
Posteriormente se realizó una reunión con el Comité Informático, encabezado por el Director del Área Informática, con el fin de realizar la selección de los procesos y que el MTOP pueda beneficiarse al máximo del resultado de la Auditoría.

Finalmente se realizó una tabla que resume todo el proceso en: Dominio de COBIT, Proceso de COBIT, Práctica Clave del Proceso de COBIT y Norma de la NCI 410 que puede ser evaluada con el respectivo Proceso de COBIT.

A continuación, en la Tabla 2 - Selección de los Dominios y Procesos de COBIT 5, tenemos un extracto de la tabla realizada para seleccionar los procesos. Los procesos seleccionados son los coloreados, los demás están en blanco. Para ver la tabla completa diríjase al ANEXO 3.

PROCESO	DESCRIPCIÓN	Práctica (Gobierno/Gestión)Clave	Descripción	NCI ACUERDO
Evaluar, Orientar y Supervisar (EMD)				
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	EDM01.01 Evaluar el sistema de gobierno	Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	410-01 (410-03) 410-04 (410-09) 410-12 (410-13) 410-16
		EDM01.02 Orientar el sistema de gobierno	Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios,modelos para la toma de decisiones y niveles de autoridaddiseñados para el gobierno. Definir la información necesariapara una toma de decisiones informadas.	
		EDM01.03 Supervisar el sistema de gobierno	Supervisar la ejecución y la efectividad del gobierno deTI de la empresa. Analizar si el sistema de gobierno y losmecanismos implementados (incluyendo estructuras,principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.	
EDM02 Asegurar la entrega de beneficios	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables	EDM02.01 Evaluar la entrega de valor	Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor.	N/A
		EDM02.02 Orientar la optimización del valor	Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico.	
		EDM02.03 Supervisar la optimización del valor	Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI. Identificar los problemas significativos y considerar las acciones correctivas.	

Tabla 2- Selección de los Dominios y Procesos de COBIT 5[11]

[11] Fuente: Tabla creada por la autora.

En la Tabla 3 - Procesos seleccionados de COBIT 5, se listan los procesos que fueron seleccionados de COBIT 5 para la realización de la auditoría.

DOMINIO	PROCESO
Evaluar, Orientar y Supervisar (EMD)	EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno
	EDM03 Asegurar la optimización del riesgo
	EDM04 Asegurar la optimización de recursos
Alinear, Planear y Organizar (APO)	APO01 Gestionar el marco de gestión de TI
	APO02 Gestionar la estrategia
	APO07 Gestionar los recursos humanos
	AP012 Gestionar el riesgo
	AP013 Gestionar la seguridad
Construir, Adquirir e Implementar (BAI)	BAI05 Gestionar la introducción del cambio organizativo
	BAI09 Gestionar los activos
Entregar, dar Servicio y Soporte (DSS)	DSS01 Gestionar operaciones
	DSS04 Gestionar la continuidad
	DSS05 Gestionar servicios de seguridad

Tabla 3- Procesos seleccionados de COBIT 5

Como se puede apreciar en la tabla sólo se han seleccionado 4 de los 5 dominios:

- Evaluar, Orientar y Supervisar (EMD)
- Alinear, Planear y Organizar (APO)
- Construir, Adquirir e Implementar (BAI)
- Entregar, dar Servicio y Soporte (DSS)

El dominio que Supervisar, Evaluar y Valorar (MEA) no ha sido tomado en cuenta dentro de la selección ya que no existen muchos controles todavía implementados por la Unidad Informática, así que se le da más importancia a los procesos que van a permitir establecer las bases para un Gobierno de TI estable dentro de la empresa.

2.2 REALIZACIÓN DE LA AUDITORÍA

Para este análisis se trabaja con la herramienta Self-Assessment-Templates para COBIT 5 y el Modelo de Capacidad de los procesos de COBIT 5.

A continuación, en la Tabla 4, se detalla el modelo de capacidad con sus 6 niveles, empezando del 0 hasta el 5, y además se da una pequeña descripción sobre el significado de cada nivel. Mediante la cuantificación de estos niveles se puede conocer el estado actual de la Unidad Informática y las metas que deben cumplirse para llegar a un nivel mayor.

Nivel de capacidad	Descripción
Nivel 0 – Proceso incompleto	El proceso no está implementado o en su defecto no alcanza su objetivo. No existe ninguna evidencia de ningún logro del proceso.
Nivel 1 – Proceso ejecutado	El proceso alcanza su propósito. (1 atributo)
Nivel 2 – Proceso gestionado	El proceso ya está implementado y gestionado (planificado, supervisado y ajustado). Los resultados están establecidos, controlados y mantenidos. (2 atributos)
Nivel 3 – Proceso establecido	El proceso gestionado está implementado usando un proceso definido que permite alcanzar sus resultados de proceso. (2 atributos)
Nivel 4 – Proceso predecible	El proceso establecido antes se ejecuta dentro de los límites definidos y permite alcanzar los resultados de proceso. (2 atributos)
Nivel 5 – Proceso optimizado	El proceso predecible es mejorado continuamente para cumplir con las metas empresariales. (2 atributos)

Tabla 4- Modelo de Capacidad

Los niveles de logro de los procesos son:

- No alcanzado: (0-15%)
- Parcialmente alcanzado: (15% -50%)
- Ampliamente alcanzado (50% - 85%)
- Completamente alcanzado (85-100%)

Como para esta Auditoría se usará la herramienta Self-Assessment-Templates para COBIT 5, en la Tabla 5 - Estructura general de SELF ASSESMENT TEMPLATE se muestra la estructura de las tablas:

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
Nivel de Capacidad	**Atributo o atributos con los que debe cumplir el proceso**	Resultados que deben ser alcanzados para el nivel	**Valor promedio**	Observación
		Resultado 1	Valor 1	
		Resultado 2	Valor 2	
		…	…	
		Resultado n	Valor n	

Tabla 5- Estructura general de SELF ASSESMENT TEMPLATE[12]

El objetivo de la Tabla 5- Estructura general de SELF ASSESMENT TEMPLATE es ilustrar la forma en la que se muestra la información, esta tabla está basada en la hoja de cálculo de la herramienta, sin embargo ha sido alterada para el presente documento.

En la primera columna se encuentra el nivel de capacidad del proceso, en la segunda el atributo, o los atributos que se evalúan en la herramienta. En la tercera columna se encuentra el resultado con el que debe cumplir el proceso, si es que lo hace. En la cuarta está el porcentaje de cumplimiento del proceso para el resultado, para el porcentaje de cumplimiento de un nivel se promedia esos valores. Finalmente, la última columna es para las observaciones en caso de que existiera alguna.

Para mayor detalle sobre los valores que están presentes en Porcentaje de Cumplimiento, ir al Anexo 4

[12] Fuente: Autora

2.2.0 ANÁLISIS DE VULNERABILIDADES CON LA HERRAMIENTA MSAT.

Previo al análisis usando COBIT se presentan los resultados obtenidos utilizando la herramienta MSAT para encontrar las vulnerabilidades del área de TI del MTOP, para mayor información sobre los resultados obtenidos y mejores prácticas consulte el Anexo 5.

Esta herramienta nos permite evaluar la Distribución de Defensa de Riesgos, a continuación se muestran los resultados obtenidos en la Figura 6.

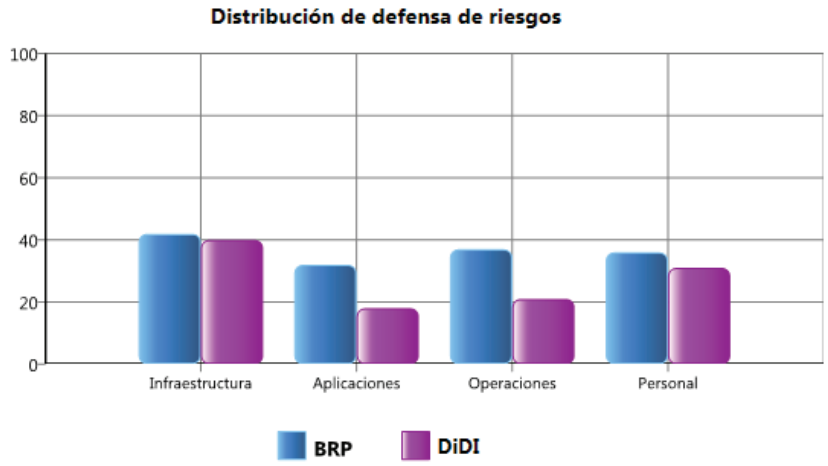


Figura 6 – Distribución de defensa de los riesgos[13]

En la figura podemos observar los resultados obtenidos para el Perfil de Riesgos del Negocio (BRP) y el Índice de Defensa a Profundidad (DiDI) para las siguientes áreas:

- Personal
- Operaciones
- Aplicaciones
- Infraestructura.

El BRP es un índice que se califica de 0 a 100, una mayor calificación significa mayor riesgo y una puntuación de 0 es imposible.

[13] Fuente: Informe de la herramienta MSAT

El DiDI también se califica de 0 a 100, una mayor calificación significa que se han tomado medidas de defensa de seguridad.

En la figura 7, tenemos la Distribución de defensa de los riesgos y madurez de la seguridad.

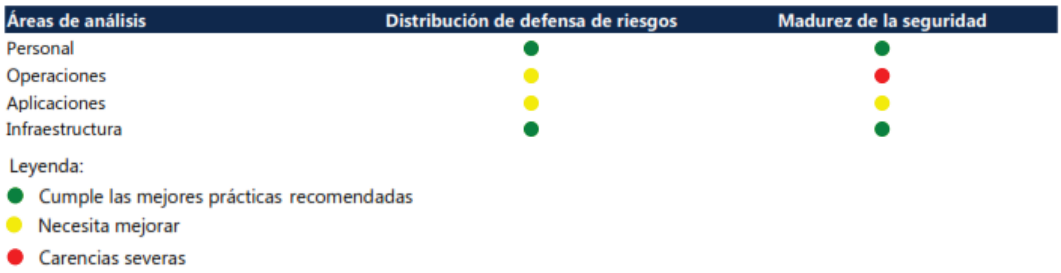


Figura 7 – Distribución de defensa de los riesgos y madurez de la seguridad[14]

En este gráfico podemos apreciar un resumen de las fortalezas y carencias del MTOP en las cuatro áreas evaluadas. Las áreas de Operación y Aplicaciones requieren más atención en este momento, tanto en distribución de defensa de riesgos y madurez de la seguridad.

A continuación se especifica detalla los puntos en los que se necesita mejorar y en los que se deben mantener las prácticas realizadas.

Para la interpretación de los resultados obtenidos con la herramienta vamos a utilizar la leyenda de la Figura 8:

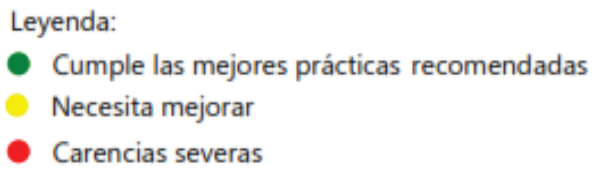


Figura 8 – Leyenda para interpretar los resultados obtenidos con MSAT[15]

[14] Fuente: Informe de la herramienta MSAT
[15] Fuente: Informe de la herramienta MSAT

Infraestructura:

El área de Infraestructura tiene carencias severas, en la figura 9 podemos observar la puntuación de cada uno de los aspectos evaluados dentro del área.

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Figura 9 – Resultados de Infraestructura[16]

A continuación se detallan los resultados obtenidos con la herramienta:

- Defensa del perímetro
    - Reglas y filtros de cortafuegos:
        - Se han instalado cortafuegos

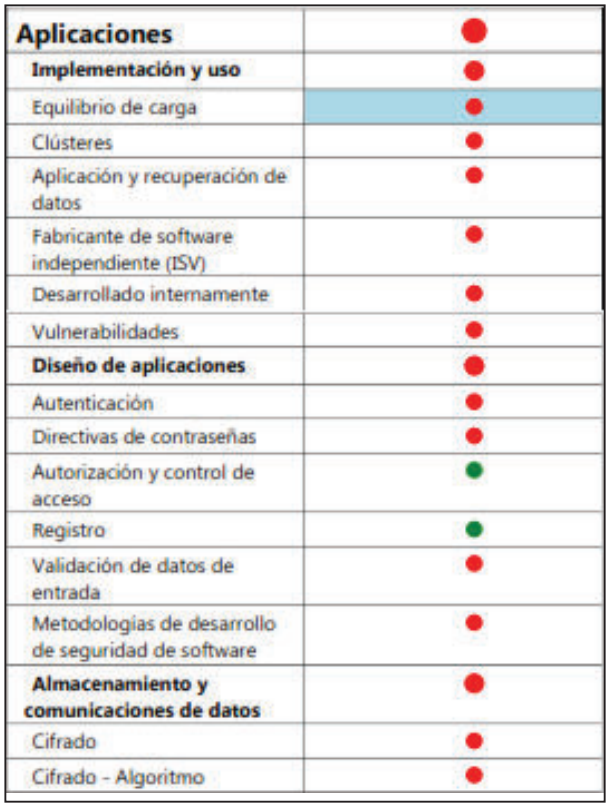
[16] Fuente: Informe de la herramienta MSAT

        - No se ha creado un segmento DMZ para proteger recursos corporativos del acceso a Internet por dispositivos internos de la empresa
        - No se monitorea el funcionamiento del cortafuegos
    - Antivirus:
        - Se utiliza antivirus
    - Antivirus - Equipos de escritorio:
        - Se utiliza antivirus en los equipos de escritorio
    - Antivirus - Servidores:
        - Se utilizan antivirus en los servidores
    - Acceso remoto:
        - No se utiliza VPN para la conexión remota de empleados y usuarios
    - Segmentación:
        - La red presenta más de un segmento
    - Sistema de detección de intrusiones:
        - No se utiliza ningún hardware ni software de detección de intrusiones
    - Inalámbrico:
        - Existe conexión inalámbrica a la red
        - Se ha modificado el SSID en el punto de acceso
        - Existe cifrado WPA
        - Se utiliza restricción por MAC
- Autenticación
    - Usuarios administrativos:
        - Se utilizan inicios de sesión distintos para la administración de seguridad de los sistemas y dispositivos del entorno.
        - Los usuarios no tienen habilitados accesos administrativos en sus dispositivos finales
    - Usuarios internos:
        - Los usuarios utilizan contraseñas para sus dispositivos finales y acceso a la red
    - Usuarios de acceso remoto:

        - Empleados, contratistas y usuarios pueden conectarse de forma remota
    - Directivas de contraseña:
        - No existen controles formales para la administración de contraseñas
- Gestión y Control
    - Informes sobre incidentes y respuesta:
        - Se crean informes sobre incidentes y respuesta.
    - Creación segura:
        - Se han instalado cortafuegos.
        - Los procesos de creación de dispositivos están documentados.
        - Se utiliza algún software de control/gestión remota en el entorno.
    - Seguridad física:
        - Existen controles de seguridad física para proteger los activos de la empresa.
        - No se ha instalado ningún sistema de alarma para detectar ni informar de intrusiones
        - Está implementado: tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes y controles de entrada
        - Los equipos de la red se hallan en una habitación cerrada con acceso restringido.
        - Las estaciones de trabajo y portátiles no están protegidas con cables de seguridad.
        - Los documentos confidenciales impresos no se guardan bajo llave.

Aplicaciones

El área de Aplicaciones tiene carencias severas, en la figura 10 podemos observar la puntuación de cada uno de los aspectos evaluados dentro del área.



Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Figura 10 – Resultados de Aplicaciones[17]

A continuación se detallan los resultados obtenidos con la herramienta:

- Implementación y uso
  - Equilibrio de carga :
    - No se utilizan equilibradores de carga en el entorno
  - Clústeres
    - No se utiliza la agrupación de clústeres en el entorno
  - Aplicación y recuperación de datos

[17] Fuente: Informe de la herramienta MSAT

        - No se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.
    - Fabricante de software independiente (ISV):
        - Otros fabricantes han desarrollado una o más de las aplicaciones principales del entorno.
    - Desarrollado internamente:
        - No se usan macros personalizadas en las aplicaciones ofimáticas.
    - Vulnerabilidades:
        - Actualmente no se conocen vulnerabilidades del entorno
- Diseño de aplicaciones
    - Autenticación:
        - Se utilizan medios de autenticación
    - Directivas de contraseñas :
        - Se usan controles de contraseña en las aplicaciones principales
    - Autorización y control de acceso :
        - Se limita el acceso a datos y funciones confidenciales según los privilegios de la cuenta.
    - Registro:
        - Hay varios eventos registrados por las aplicaciones del entorno: intentos fallidos de autenticación, intentos de autenticación correctos, errores de las aplicaciones, accesos denegados a los recursos, accesos correctos a los recursos
    - Validación de datos de entrada:
        - No se usan mecanismos para validar los datos de entrada en las aplicaciones del entorno.
- Almacenamiento y comunicaciones de datos
    - Cifrado:
        - Las aplicaciones no cifran los datos cuando están almacenados o se están transmitiendo.

Operaciones

El área de Operaciones tiene carencias severas, en la figura 11 podemos observar la puntuación de cada uno de los aspectos evaluados dentro del área.

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Figura 11 – Resultados de Operaciones[18]

A continuación se detallan los resultados obtenidos con la herramienta:

- Directiva de seguridad
  - Clasificación de datos
    - Los datos no se clasifican

[18] Fuente: Informe de la herramienta MSAT

    - Eliminación de datos
        - No se tienen políticas para la correcta eliminación de los datos
    - Gestión de cuentas de usuarios:
        - Se gestionan las cuentas de usuario
- Gestión de actualizaciones y revisiones
    - Documentación de la red:
        - No existe documentación de la red
    - Flujo de datos de la aplicación
        - No se analiza el flujo de datos de la aplicación
    - Gestión de actualizaciones
        - No se realizan actualizaciones fuera de las del Sistema Operativo
    - Gestión de cambios y configuración
        - No se gestionan los cambios.
- Copias de seguridad y recuperación
    - Archivos de registro:
        - Se tienen archivos de registro.
    - Planificación de recuperación ante desastres y reanudación de negocio:
        - No se tiene un plan de recuperación de desastres ni un plan de reanudación del negocio
    - Copias de seguridad
        - No se generan ni administran copias de seguridad

Personal

El área de Personal tiene carencias severas, en la figura 12 podemos observar la puntuación de cada uno de los aspectos evaluados dentro del área.

Figura 12 – Resultados de Personal[19]

A continuación se detallan los resultados obtenidos con la herramienta:

- Requisitos y evaluaciones
  - Requisitos de seguridad:
    - El MTOP tiene un modelo para la asignación de niveles de gravedad a cada componente del entorno informático.
    - Existen equipos comerciales y de seguridad que trabajan definiendo requisitos de seguridad.
  - Evaluaciones de seguridad:
    - No se realizan evaluaciones de seguridad
- Directiva y procedimientos
  - Comprobaciones del historial personal :
    - Se comprueba el historial personal de todos los empleados.
  - Directiva de recursos humanos:
    - No existe ninguna directiva formal para los empleados que dejan la empresa.

[19] Fuente: Informe de la herramienta MSAT

- Relaciones con terceros:
  - Los sistemas se configuran por parte de personal interno.
  - El Ministerio gestiona el entorno informático.
  - No existe ninguna directiva para las relaciones con terceros.

- Formación y conocimiento
  - Conocimiento de seguridad:
    - Se ha creado y asignado al personal encargado de la seguridad para definir requisitos tanto para la tecnología nueva como existente.
    - No existe ningún programa de divulgación de las medidas de seguridad en la empresa.
  - Formación sobre seguridad:
    - La empresa no ofrece actualmente a los empleados formación específica por temas.

Iniciativas de Seguridad

Según el análisis realizado con la herramienta MSAT, las áreas que se detallan en la figura 13 no cumplen con las mejores prácticas y deben ser trabajadas con prioridad alta, intermedia y baja.

Prioridad alta	Prioridad intermedia	Prioridad baja
• Usuarios de acceso remoto	• Seguridad física	• Antivirus - Equipos de escritorio
• Acceso remoto	• Inalámbrico	• Antivirus - Servidores
• Segmentación	• Conocimiento de seguridad	• Autorización y control de acceso
• Creación segura	• Reglas y filtros de cortafuegos	• Regulación
• Relaciones con terceros	• Cuentas inactivas	• Directiva de seguridad

Figura 13 – Iniciativas de Seguridad[20]

[20] Fuente: Informe de la herramienta MSAT

A continuación se detallan los procesos analizados y los resultados encontrados:

2.2.1 EDM01 ASEGURAR EL ESTABLECIMIENTO Y MANTENIMIENTO DEL MARCO DE REFERENCIA DE GOBIERNO

Descripción del Proceso: "Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa."[21]

Práctica: EDM01.01 Evaluar el sistema de gobierno

Descripción: "Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa."[22]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se tienen reconocidas las obligaciones legales, contractuales y regulatorias para la Unidad Informática que influyen sobre el diseño del gobierno, las normas que deben aplicarse para la UI del MTOP están definidas, entre ellos tenemos el acuerdo 166, la norma 410 para TI del acuerdo 039 NCI y el Estatuto Orgánico de Gestión Organizacional por procesos
- La relevancia de la Unidad de TI en el MTOP es menor a lo recomendado, es un proceso de apoyo en lugar de ser un proceso principal
- Las regulaciones externas se encuentran analizadas, pero aún no han sido implementadas, se implementarán desde el año 2015

[21] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 31
[22] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 32.

- En las normas vienen determinados los controles que se deben aplicar para el área de TI

Práctica: EDM01.02 Orientar el sistema de gobierno

Descripción: "Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas."[23]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se ha conformado un comité para establecer un sistema de gobierno de la información, con responsables y roles bien definidos, sin embargo las reuniones son escasas, 4 veces en el último año.
- No se tienen buenos sistemas de comunicación para la obtención y socialización de la información relevante.

Práctica: EDM01.03 Supervisar el sistema de gobierno

Descripción: "Supervisar la ejecución y la efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI."[24]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Sólo se encuentra definido el comité pero aún no se ha implementado un sistema de gobierno de TI.

[23] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 32.
[24] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 33.

En la Tabla 6- Nivel de Capacidad Proceso EDM01: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno, se realiza un análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**0**	Existe la necesidad de establecer un sistema de gobierno que esté integrado y alineado al MTOP sin embargo no está implementado.
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**0**	
		El modelo de toma de decisiones estratégicas para TI es efectivo y está alineado con el ambiente interno y externo de la empresa, y los requerimientos de los skateholders.	0	
		El sistema de gobierno de TI está embebido en la empresa	0	
		Se tiene la seguridad de que el sistema de gobierno de TI opera efectivamente.	0	

Tabla 6- Nivel de Capacidad Proceso EDM01: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno[25]

2.2.2 EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO

Descripción del Proceso: "Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.**"**[26]

Práctica: EDM03.01 Evaluar la gestión de riesgos

Descripción: **"**Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo

[25] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[26] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 39.

de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado.”[27]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP reconoce la necesidad de identificar los riesgos, sin embargo no se tiene un análisis de riesgo, tampoco se conoce el apetito del riesgo y no se gestionan los riesgos en ninguna forma.

Práctica: EDM03.02 Orientar la gestión de riesgos

Descripción: **“**Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.”[28]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- En el MTOP no se gestionan los riesgos.

Práctica: EDM03.03 Supervisar la gestión de riesgos

Descripción: **“**Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.” [29]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- En el MTOP no se gestionan los riesgos por lo tanto no se supervisa la gestión de riesgos.

[27] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 40.
[28] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 40.
[29] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 41.

En la Tabla 7- Nivel de Capacidad Proceso EDM03: Asegurar la optimización del riesgo, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**0**	El MTOP no ha realizado ningún análisis de riesgo, sin embargo conoce de la necesidad del análisis de riesgo. A implementarse desde el 2015
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**0**	
		Los umbrales de riesgo están definidos y son comunicados. Los riesgos relativos a TI son conocidos.	0	
		La empresa maneja el riesgo crítico relacionado a las TI de manera efectiva y eficiente.	0	
		El riesgo empresarial relacionado a las TI no excede el apetito de riesgo y el impacto del riesgo de TI es identificado y gestionado.	0	

Tabla 7- Nivel de Capacidad Proceso EDM03: Asegurar la optimización del riesgo [30]

2.2.3 EDM04 ASEGURAR LA OPTIMIZACIÓN DE RECURSOS

Descripción del Proceso: "Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo."[31]

Práctica: EDM04.01 Evaluar la gestión de recursos

Descripción: "Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de

[30] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[31] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 43.

asignación y gestión para cumplir de manera óptima con las necesidades de la empresa."[32]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se realiza inventarios, proyecciones y análisis de crecimiento de capacidad a futuro, teniendo en cuenta el presupuesto.
- Se evalúa y analiza la capacidad actual y futura de la empresa en conjunto con talento humano y el área administrativa

Práctica: EDM04.02 Orientar la gestión de recursos

Descripción: "Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica"[33]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se comunica e impulsa la adopción de estrategias de gestión de recursos.
- No se tienen objetivos de desempeño, sin embargo se realiza inventario periódicamente, se han definido responsables para los activos y los inventarios.
- No se tienen principios ni políticas para la protección de recursos.

Práctica: EDM04.03 Supervisar la gestión de recursos

Descripción: "Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas."[34]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Cada año se hace un análisis de la necesidad de recursos, pero no se tienen objetivos ni métricas para la gestión de recursos establecidos.

[32] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 44.
[33] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 44.
[34] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 44.

En la Tabla 8- Nivel de Capacidad Proceso EDM03: Asegurar la optimización de recursos, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**100**	Se realiza inventarios, proyecciones, análisis de crecimiento de capacidad a futuro, presupuesto, en conjunto con Talento Humano y el área Administrativa
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**70**	
		Las necesidades empresariales de recursos son reconocidas con capacidades óptimas.	50	Se realiza inventarios, proyecciones, análisis de crecimiento de capacidad a futuro, presupuesto
		Los recursos son asignados para cumplir las prioridades empresariales dentro de las limitaciones presupuestarias.	80	El análisis de inventarios se realiza en conjunto con Talento Humano, y también con el área administrativa
		Se logra un óptimo uso de los recursos a lo largo de su ciclo de vida.	80	Se utilizan los equipos hasta cumplir con su ciclo de vida
2 PROCESO GESTIONADO	**Gestión de rendimiento: Una medida del grado en el que se gestiona el rendimiento del proceso**	**Como resultado del completo alcance de este atributo:**	**13**	
		a) Se identifican los objetivos para el rendimiento del proceso	0	No se tienen objetivos de desempeño, sin embargo se realiza inventario periódicamente, se han definido responsables para los activos y los inventarios.
		b) El rendimiento del proceso es planeado y monitoreado	0	
		c) El rendimiento de los procesos se ajusta para cumplir con los planes	0	
		d) Las responsabilidades y autoridades para el rendimiento del proceso son definidos, asignados y comunicados	50	
		e) Los recursos y la información necesarios para el rendimiento del proceso son identificados, disponibilizados, localizados y usados	25	
		f) Las interfaces entre las partes envueltas se gestionan para	0	

		asegurar comunicación efectiva y una clara asignación de responsabilidad.		
	Gestión de producto de trabajo: Una medida del grado en que los productos de trabajo producidos por el proceso se gestionan correctamente. Los productos de trabajo se definen y controlan	**Como resultado del completo alcance de este atributo:**	**0**	
		a) Los requerimientos para los productos de trabajo del proceso son definidos.	0	Los inventarios no están apropiadamente identificados, documentados y controlados.
		b) Los requerimientos para documentación y control de los productos de trabajo son definidos.	0	
		c) Los productos de trabajo son apropiadamente identificados, documentados y controlados.	0	
		d) Los productos de trabajo son revisados de acuerdo a los arreglos planeados y ajustados de acuerdo a la necesidad para cumplir con requerimientos.	0	

Tabla 8- Nivel de Capacidad Proceso EDM04: Asegurar la optimización de recursos[35]

2.2.4 APO01 GESTIONAR EL MARCO DE GESTIÓN DE TI

Descripción del Proceso: "Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores."[36]

Práctica: APO01.01 Definir la estructura organizativo

Descripción: "Establecer una estructura organizativo interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las

[35] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[36] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 51

estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible."[37]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP nota la necesidad de definir el alcance, roles, capacidades y funciones, tanto internas como externas, pero aún no se ha definido aspectos de la arquitectura, se tiene un comité de tecnologías de la información pero falta definir la estructura

Práctica: APO01.02 Establecer roles y responsabilidades

Descripción: "Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante."[38]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se establece, acuerda y comunica roles y responsabilidades relativos a TI para todo el personal de la empresa.
- No se tiene en cuenta la continuidad del servicio de TI.
- Se tienen roles y responsabilidades definidos pero aún no están adheridos a las políticas.

Práctica: APO01.03 Mantener los elementos catalizadores del sistema de gestión

Descripción: "Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación

[37] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 52
[38] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 53

interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos)."[39]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Las TI se alinean con estándares y códigos, aunque no se hallan implementados.
- No se comprende la visión, dirección y estrategias corporativas, cultura empresarial o filosofía de gestión.

Práctica: APO01.04 Comunicar los objetivos y la dirección de gestión

Descripción: "Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas y usuarios pertinentes a lo largo de toda la empresa."[40]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Los objetivos se comunican mediante correos, no existen otros medios de comunicación para todos los usuarios.

Práctica: APO01.05 Optimizar la ubicación de la función de TI

Descripción: "Posicionar la capacidad de TI en la estructura organizativo global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. La línea de reporte del CIO debe ser proporcional a la importancia de las TI en la empresa."[41]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- LA UI no se encuentra en un lugar óptimo, es un proceso de apoyo en lugar de ser un proceso principal

[39] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 54
[40] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 54
[41] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 55

Práctica: APO01.06 Definir la propiedad de la información (datos) y del sistema

Descripción: "Definir y mantener las responsabilidades de la propiedad de la información (datos) y los sistemas de información. Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación."[42]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tienen políticas para la clasificación de la información, no se tienen inventarios de la información ni se garantiza la seguridad

Práctica: APO01.07 Gestionar la mejora continua de los procesos

Descripción: "Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso."[43]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se realizan mejoras continuas.

Práctica: APO01.08 Mantener el cumplimiento con las políticas y procedimientos

Descripción: "Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del

[42] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 55
[43] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 55

desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control."[44]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Aún no se implementa o monitorea políticas y procedimientos.

En la Tabla 9- Nivel de Capacidad Proceso APO01: Gestionar el marco de gestión de TI , se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**100**	El MTOP reconoce la necesidad de estructuras organizacionales, roles y responsabilidades, actividades confiables y repetibles, y habilidades y competencias. Sin embargo aún no se tienen implementadas las actividades de este proceso.
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**25**	
		Un conjunto efectivo de políticas ha sido definido y mantenido.	50	Las políticas han sido definidas, sin embargo aún no se han implementado
		Todos están al tanto de las políticas y como deberían ser implementadas.	0	No se han implementado ni comunicado.

Tabla 9- Nivel de Capacidad Proceso APO01: Gestionar el marco de gestión de TI[45]

2.2.5 APO02 GESTIONAR LA ESTRATEGIA

Descripción del Proceso: "Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos."[46]

[44] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 56
[45] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[46] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 57

Práctica: APO02.01 Comprender la dirección de la empresa

Descripción: "Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella (motivadores de la industria, reglamentos relevantes, bases para la competencia)"[47]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP entiende la necesidad de establecer un entendimiento del entorno interno y externo de la empresa, partes interesadas y necesidad de cambio, y se plantea la necesidad de cambio aunque no se tiene documentada más que en los reglamentos.

Práctica: APO02.02 Evaluar el entorno, y rendimiento actuales

Descripción: **"**Evaluar el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Identificarlos problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos.**"**[48]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- La UI no establece controles para los servicios externos de TI y las revisiones internas se realizan raramente. No se identifican los riesgos del servicio.

Práctica: APO02.03 Definir el objetivo de las capacidades de TI

Descripción: **"**Definir el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del

[47] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 58
[48] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 59

entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación.”[49]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Aún se deben realizar análisis sobre el objetivo del negocio y como la UI puede ayudar al MTOP a cumplirlo, además se necesita una mejor comprensión sobre la importancia del uso de los servicios de TI. No se considera la aprobación de tecnologías emergentes. Tampoco se tienen análisis sobre tecnologías actuales.

Práctica: APO02.04 Realizar un análisis de diferencias

Descripción: **“**Identificar las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia.”[50]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El análisis de diferencias ayuda a mejorar el entendimiento de la situación actual y la situación deseada. A continuación se indica un ejemplo de un análisis de diferencias teniendo en cuenta la Norma 410 del Acuerdo 039 – Normas de Control Interno:

[49] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 60
[50] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 60

	Entorno deseado	Entorno Actual
Organización Informática	Trabajar en base a un marco de trabajo que asegure transparencia, control e involucre la alta dirección. Estar posicionada en un nivel gerencial en la estructura organizacional y no depender de otras áreas. Establecer revisiones periódicas de la estructura organizacional para ajustar estrategias y cumplir objetivos	Aún no se aplica
Segregación de funciones	Ser definidos claramente y formalmente comunicados, asegurándose de que exista suficiente autoridad y respaldo. Ser documentados teniendo en cuenta deberes, responsabilidades, habilidades y experiencia necesarios para cada posición.	Los roles son definidos informalmente, sin la documentación adecuada.
Plan informático estratégico de tecnología	Elaborar un plan informático estratégico alineado con el plan estratégico institucional que contenga e incluir análisis de la situación actual y propuestas de mejora.	Aún no se tiene elaborado el plan ni algún otro plan.
Políticas y procedimiento	Ser definidos, documentados, difundidos y actualizados permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que	Las políticas son documentadas a nivel ministerial, no de unidad. Los procedimientos no son documentados.

	hubiere lugar si no se cumplieran. Implementar planes para monitorear y medir el cumplimiento con indicadores de desempeño.	No se tienen planes para monitorear y medir el cumplimiento de indicadores de desempeño.
Modelo de información organizacional	Garantizar la disponibilidad, integridad, exactitud y seguridad de la información. Incluir reglas de validación, controles de integridad y consistencia de los datos Clasificar los datos para especificar y aplicar niveles de seguridad.	No se tienen controles para la información.
Administración de proyectos tecnológicos	Documentar los proyectos tecnológicos. Realizar un cronograma de actividades que incluya responsables, recursos y contemple pruebas y capacitación. Monitorear avances del proyecto Incluir análisis de riesgos, control de cambios y un plan para el aseguramiento de la calidad.	No se tiene documentación sobre administración de proyectos tecnológicos, los avances se verifican informalmente y por correo.
Desarrollo y adquisición del software aplicativo	Documentar los proyectos de desarrollo y adquisición de Software. Realizar un cronograma de actividades que incluya responsables, recursos y contemple pruebas y	No se tiene documentación sobre administración de proyectos tecnológicos, los avances se verifican informalmente y por correo.

	capacitación. Monitorear avances del proyecto Incluir análisis de riesgos, control de cambios y un plan para el aseguramiento de la calidad. Iniciar etapas del proyecto con aprobaciones formales de los interesados.	No se realiza análisis de riesgo o planes para el aseguramiento de la calidad.
Adquisiciones de infraestructura tecnológica	Realizar un análisis documentado de la necesidad de adquisiciones tecnológicas Planificar el incremento de capacidad, evaluar riesgos tecnológicos, costos, vida útil considerando los requerimientos de la carga laboral. Detallar los contratos sobre características técnicas de los equipos adquiridos.	La UI del MTOP realiza inventarios de los equipos y además realizan un análisis de adquisiciones tecnológicas conjuntamente con el área administrativa.
Mantenimiento y control de infraestructura tecnológica	Definir procedimientos para el uso y mantenimiento adecuado de la infraestructura tecnológica. Definir procedimientos para mantenimiento, despliegue, corrección y mejoramiento de software y documentar los cambios. Controlar y registrar las versiones de software. Actualizar y difundir manuales técnicos y de usuario según	Se tienen procedimientos no documentados para el mantenimiento de la infraestructura tecnológica. Las actividades son del día al día. No se tienen procedimientos documentados, manuales técnicos, planes de mantenimiento.

	los cambios. Elaborar planes de mantenimiento preventivo y correctivo, y realizar revisiones periódicas, sobre todo de las aplicaciones críticas de la organización. Realizar inventario de bienes informático detallado.	Se tienen inventarios.
Seguridad de tecnología de la información	Establecer una ubicación adecuada con control de acceso físico a la unidad de tecnologías de la información, tener en cuenta mecanismos de control de incendios, temperatura y humedad adecuadas, entre otros. Respaldar la información periódicamente. Respaldar la información en medios físicos adecuados en caso de actualización. Almacenar los respaldos con información crítica en lugares externos a la organización Implementar seguridades para software y hardware, establecer monitoreos de seguridad, pruebas periódicas y acciones correctivas con las vulnerabilidades encontradas. Establecer sitios de procesamiento alternativos Implementar procedimientos de seguridad para el recurso humano.	Se tienen mecanismos de acceso, control de incendio, seguridad física y lógica, no documentados. No existen políticas de respaldo de la información, ni replicación de servidores. Se tienen implementadas seguridades para software y hardware, no hay monitoreos de seguridad, pruebas periódicas ni análisis de vulnerabilidades.

Plan de contingencias	Definir un plan de contingencias incluyendo los escenarios de contingencia, roles y responsabilidades. Establecer un plan de continuidad del negocio. En el plan se debe incluir el uso de un centro de cómputo. Establecer un plan de recuperación de desastres que contemple las actividades, antes, durante y después de un desastre.	No existe plan de contingencias, de continuidad del negocio ni de recuperación de desastres
Administración de soporte de tecnologías de la información	Establecer medidas de prevención, detección y corrección de software malicioso. Crear roles y perfiles de usuarios con una identificación única y estandarizada para cada usuario. Mantener un repositorio con la documentación de hardware y software actualizado, asegurar la integridad y disponibilidad de la información. Crear respaldos	Se utiliza protección antivirus en cada computador. Se tienen roles y perfiles de usuarios, sin políticas documentadas.
Monitoreo y evaluación de los procesos y servicios	Monitorear la contribución e impacto del área en el ministerio. Establecer métricas e indicadores para indicar el nivel de satisfacción de clientes internos y externos	No se realizan monitoreos para verificar la contribución del área en el ministerio.
Sitio web, servicios de internet e intranet	La unidad de tecnología de información debe elaborar políticas y procedimientos documentados sobre los servicios de Internet, intranet, correo electrónico y el sitio WEB del ministerio.	No se tienen documentadas políticas ni procedimientos.
Capacitación	Se debe establecer un plan para capacitar a los	No se tiene un plan de capacitación.

informática	empleados.	
Comité informático	La unidad informática es la encargada de crear un comité informático teniendo en cuenta el tamaño y complejidad del ministerio. La conformación y funciones del comité, su reglamentación, la creación de grupos de trabajo, la definición de las atribuciones y responsabilidades de los miembros del comité, entre otros aspectos.	Existe comité informático pero no se reúnen con regularidad. Aunque se tiene un comité informático, se debe establecer tiempos para sus reuniones, asignar roles y responsabilidades.

Tabla 10- Análisis de diferencias

En la Tabla 10- Análisis de diferencias, se realiza un contraste de la situación actual y de la situación deseada. Debe existir una transición de la primera a la segunda para poder cumplir con la normativa ecuatoriana, en las leyes se establece que todos los ministerios deben cumplir estas normas desde el 2013, desde entonces se ha analizado la viabilidad de aplicar estas normas.

Práctica: APO02.05 Definir el plan estratégico y la hoja de ruta

Descripción: "Crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel."[51]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene un plan estratégico ni hoja de ruta.

Práctica: APO02.06 Comunicar la estrategia y la dirección de TI

Descripción: "Crear conciencia y comprensión del negocio y de los objetivos y dirección de TI, como se encuentra reflejada en la estrategia de TI, a través de comunicaciones a las partes interesadas adecuadas y a los usuarios de toda la empresa."[52]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Los mensajes se transmiten básicamente por correo electrónico. No se tiene un plan de comunicaciones ni entrega.

[51] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 61
[52] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 61

En la Tabla 9- Nivel de Capacidad Proceso APO02 Gestionar la estrategia, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cum p%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**100**	El MTOP reconoce la necesidad de una estrategia de TI orientada, sin embargo aún se encuentra en desarrollo y no implementada
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**22**	
		Todos los aspectos de la estrategia de TI están alineados con la estrategia empresarial.	50	La estrategia IT se está desarrollando y aún no implementada
		La estrategia de TI es costo-efectiva, apropiada, realista, alcanzable, orientada a la empresa y balanceada	0	No se han implementado ni comunicado.
		Metas de corto plazo son claras y concretas, y trazadas a iniciativas de largo plazo específicas a ser implementadas en planes operativos.	25	
		TI tiene un valor fundamental para la empresa.	15	

Tabla 11- Nivel de Capacidad Proceso APO02 Gestionar la estrategia [53]

2.2.6 APO07 GESTIONAR LOS RECURSOS HUMANO

Descripción del Proceso: "Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo

[53] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template

personal y las expectativas de desempeño, con el apoyo de gente competente y motivada."[54]

Práctica: APO07.01 Mantener la dotación de personal suficiente y adecuada

Descripción: **"**Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos. **"**[55]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- La unidad informática no tiene suficiente autonomía para hacer contratación de personal, aunque reconocen la necesidad de aumentar el personal. No existen tampoco planes de capacitación para el nuevo personal contratado, las actividades se realizan sin procedimientos formales.
- Si se verifican antecedentes en el proceso de contratación de TI para empleados, contratistas y proveedores.

Práctica: APO07.02 Identificar personal clave de TI

Descripción: **"**Identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (Backup) del personal.**"**[56]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene seleccionado al personal clave, ni se documenta como se realizan las actividades que desempeña cada persona, las actividades

[54] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 83
[55] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 84
[56] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 85

se hacen de acuerdo a las necesidades diarias. No se tienen planes de respaldo del personal.

Práctica: APO07.03 Mantener las habilidades y competencias del personal

Descripción: **"**Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.**"**[57]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene manejo de habilidades y competencias del personal. No hay repositorios de conocimiento

Práctica: APO07.04 Evaluar el desempeño laboral de los empleados

Descripción: "Lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Los empleados deberían recibir preparación sobre el desempeño y conducta siempre que sea apropiado."[58]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se realizan evaluaciones sobre el desempeño laboral de los empleados, no se tienen objetivos individuales.

[57] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 85
[58] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 86

Práctica: APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio

Descripción: **"**Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.**"**[59]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se realizan inventarios de recursos humanos, sin embargo no se cuenta con el completo apoyo de la gerencia ministerial para poder contratar al personal necesario. A pesar de entender la demanda actual y futura de recursos humanos es sumamente difícil contratar personal.

Práctica: APO07.06 Gestionar el personal contratado

Descripción: "Asegúrese de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados."[60]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No existen políticas para gestión de consultores y proveedores.

En la Tabla 12- Nivel de Capacidad Proceso APO07 Gestionar los recursos humanos, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**0**	El MTOP reconoce la necesidad de una estrategia de TI orientada, sin embargo aún se encuentra en desarrollo y no implementada

[59] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 86
[60] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 87

1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**0**	
		La estructura organizacional y las relaciones son flexibles y responsivas.	0	A pesar de que el MTOP reconoce la necesidad de optimizar los recursos humanos no cuenta con el apoyo deseado para contratar gente en el área de TI
		Los recursos humanos son gestionados afectiva y eficientemente.	0	No se tiene un proceso de capacitación para los nuevos empleados, se maneja como una actividad del día a día

Tabla 12- Nivel de Capacidad Proceso APO07 Gestionar los recursos humanos [61]

2.2.7 AP012 GESTIONAR EL RIESGO

Descripción del Proceso: "Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa."[62]

Práctica: AP012.01 Recopilar datos

Descripción: "Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI."[63]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP no gestiona el riesgo, no mantiene un método de obtención de información ni clasificación de datos referente a los riesgos. No se tiene ningún análisis de riesgo.

Práctica: AP012.02 Analizar el riesgo

Descripción: "Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo."[64]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP no gestiona el riesgo, no se han realizado análisis de riesgo.

[61] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[62] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 107
[63] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 108
[64] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 109

Práctica: AP012.03 Mantener un perfil de riesgo

Descripción: "Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados."[65]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP no gestiona el riesgo, no se han realizado análisis de riesgo.

Práctica: AP012.04 Expresar el riesgo

Descripción: "Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada."[66]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP no gestiona el riesgo, no se han realizado análisis de riesgo.

Práctica: AP012.05 Definir un portafolio de acciones para la gestión de riesgos

Descripción: "Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio."[67]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP no gestiona el riesgo, y tampoco se han analizado acciones de respuesta al riesgo.

Práctica: AP012.06 Responder al riesgo

Descripción: "Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI."[68]

---

[65] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 110
[66] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 110
[67] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 110
[68] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 111

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El MTOP no gestiona el riesgo, no se tiene ningún plan ni documentación alguna para responder al riesgo.

En la Tabla 13- Nivel de Capacidad Proceso AP012 Gestionar el riesgo, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**0**	El MTOP reconoce la necesidad de gestionar el riesgo, sin embargo no se tiene elaborado un plan de gestión de riesgo
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**0**	
		El riesgo relativo a TI se ha identificado, analizado, gestionado y reportado.	0	No se ha analizado el riesgo de TI
		Existe un perfil de riesgo completo y actualizado	0	No existe perfil de riesgo.
		Todas las acciones significantes de gestión de riesgos son administradas y están bajo control	0	No se gestiona el riesgo.
		Las acciones de manejo de riesgos son implementadas efectivamente	0	No se gestiona el riesgo.

Tabla 13- Nivel de Capacidad Proceso AP012 Gestionar el riesgo [69]

2.2.8 AP013 GESTIONAR LA SEGURIDAD

Descripción del Proceso: "Definir, operar y supervisar un sistema para la gestión de la seguridad de la información."[70]

Práctica: AP013.01 Establecer y mantener un SGSI

Descripción: **"**Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información,

[69] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[70] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 113

tecnología y procesos de negocio que estén alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.”[71]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene SGSI definido.
- La Unidad Informática del MTOP sin embargo maneja los siguientes aspectos relacionados a la seguridad informática.

SEGURIDAD FÍSICA

En lo que refiere a seguridad física, existe un personal de guardia privada en la entrada del edificio, el mismo que verifica que no se ingrese material potencialmente inseguro, así como verificar quien ingresa y cuál es su propósito dentro de las instalaciones, en el octavo piso donde se encuentra la Unidad de Información existe otro guardia que cuida la entrada a la unidad de información. La seguridad de la unidad de información consiste en una puerta que solo se abre un una tarjeta magnética o identificarse con el guardia. La puerta siempre está cerrada. Dentro de las instalaciones existen extintores en caso de incendios y tienen planes de escape en una posible emergencia.

En lo que se refiere a los servidores, el personal no interactúa directamente con ellos sino que lo hace desde conexiones remotas, los servidores se encuentran es salas frías, esta sala está a cargo del personal autorizado.

SEGURIDAD LÓGICA

Existen perfiles de usuario y contraseñas para el personal autorizado encargado de algún servidor. No existen políticas para el manejo de contraseñas.

SEGURIDAD LEGAL

Las licencias de software que manejan los ordenadores no son originales, sólo las de los sistemas operativos vienen instaladas de fábrica.

[71] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 114

SEGURIDAD DE DATOS

El MTOP no tiene planes de contingencia, respaldo sino que toda la información se almacena en los servidores localizados en este mismo edificio.

Práctica: AP013.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información

Descripción: **"**Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.**"**[72]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tienen análisis de riesgo de la seguridad de la información.

Práctica: AP013.03 Supervisar y revisar el SGSI

Descripción: "Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua."[73]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene un SGSI establecido.

[72] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 115
[73] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 115

En la Tabla 14- Nivel de Capacidad Proceso AP013 Gestionar la seguridad, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**0**	El MTOP reconoce la necesidad de gestionar la seguridad, aunque no hay plan de seguridad, pero se realizan procedimientos de seguridad del día a día.
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**0**	
		El riesgo relativo a TI se ha identificado, analizado, gestionado y reportado.	0	No se ha analizado el riesgo de TI
		Existe un perfil de riesgo completo y actualizado	0	No existe perfil de riesgo.
		Todas las acciones significantes de gestión de riesgos son administradas y están bajo control	0	No se gestiona el riesgo.
		Las acciones de manejo de riesgos son implementadas efectivamente	0	No se gestiona el riesgo.

Tabla 14- Nivel de Capacidad Proceso AP013 Gestionar la seguridad[74]

2.2.9 BAI05 GESTIONAR LA INTRODUCCIÓN DEL CAMBIO ORGANIZATIVO

Descripción del Proceso: "Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI."[75]

Práctica: BAI05.01 Establecer el deseo de cambiar

Descripción: "Comprender el alcance e impacto del cambio divisado y la disposición/voluntad de cambiar de las partes interesadas. Identificar las acciones para motivar a las partes interesadas para aceptar y querer que el cambio sea exitoso."[76]

[74] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[75] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 145
[76] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 146

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se tiene establecido el deseo de cambiar, aunque no se tiene documentado nada, no se han realizado análisis sobre los conflictos que podrían producirse. El cambio es una impulsado por necesidad legal.
- El deseo de cambio ha sido entendido pero aún no se tiene todo el apoyo para producirse.

Práctica: BAI05.02 Formar un equipo de implementación efectivo

Descripción: "Establecer un equipo de implementación efectivo, con miembros adecuados, creando confianza y estableciendo metas comunes y medidas efectivas."[77]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se ha formulado un equipo competente, que por sus diversas actividades debido a la falta de personal están obligados a retrasar el cambio.

Práctica: BAI05.03 Comunicar la visión deseada

Descripción: "Comunicar la visión deseada para el cambio en el lenguaje de aquellos que se verán afectados. La comunicación debería ser realizada por la alta dirección e incluir la razón de ser y los beneficios del cambio, el impacto de no hacerlo y la visión, la hoja de ruta y la participación requerida de las diversas partes interesadas."[78]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- La comunicación se hace básicamente por correos electrónicos. El cambio se produce por necesidad legales pero no se ha profundizado en comunicar las ventajas que tiene la implantación del cambio. Es necesario el cambio para cumplir con las leyes del país.

[77] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 147
[78] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 147

Práctica: BAI05.04 Facultar a los que juegan algún papel e identificar ganancias en el corto plazo

Descripción: "Facultar a aquellos con roles en la implementación asegurando que se han asignado responsabilidades, se ha dado formación y se han alineado las estructuras organizativas y procesos de RRHH. Identificar y comunicar ganancias en el corto plazo que pueda ser realizadas y resulten importantes desde una perspectiva de posibilitar el cambio."[79]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Aún no están empoderados para ejercer el cambio.
- No se ha planificado las necesidades de formación de personal para responder al cambio, no se ha hecho un análisis de cambio teniendo en cuenta al talento humano.

Práctica: BAI05.05 Facilitar la operación y el uso

Descripción: "Planificar e implementar todos los aspectos técnicos, operativos y de modo de uso de forma que todos aquellos involucrados en el entorno futuro puedan ejercer sus responsabilidades."[80]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se ha desarrollado un plan de operación y uso del cambio.

Práctica: BAI05.06 Integrar nuevos enfoques

Descripción: "Integrar nuevos enfoques mediante el seguimiento de los cambios implementados, asegurando la efectividad del plan de operación y uso y manteniendo un plan de concienciación mediante comunicaciones regulares. Aplicar las medidas correctoras que se estime apropiado y que podrían incluir el forzar el cumplimiento."[81]

---

[79] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 147
[80] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 148
[81] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 148

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se ha realizado seguimiento de cambios implementados, ni se han desarrollado planes que permitan facilitar y asegurar el cambio.

Práctica: BAI05.07 Mantener los cambios

Descripción: "Mantener los cambios mediante la formación eficaz del personal nuevo, campañas de comunicación periódicas, compromiso de la alta dirección, supervisión de la adopción de los cambios y divulgación a toda la empresa de las lecciones aprendidas."[82]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- El cambio se da por disposiciones legales y debe ser mantenido, se toma más como una imposición que como un compromiso.

En la Tabla 15- Nivel de Capacidad Proceso BAI05 Gestionar la introducción del cambio organizativo, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**100**	El MTOP está en un proceso de cambio organizativo, se tiene clara la necesidad del cambio y se ha implementado un equipo para lograr la transición.
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**40**	
		El deseo de cambio ha sido entendido.	80	El deseo de cambio ha sido entendido pero aún no se tiene todo el apoyo para producirse.
		El equipo de implementación es competente y capaz de dirigir el cambio.	80	Se ha formulado un equipo competente, que por sus diversas actividades debido a la falta de personal están obligados a retrasar el cambio.

[82] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 148

		El deseo de cambio ha sido entendido y aceptado por los skateholders.	50	Es necesario el cambio para cumplir con las leyes del país.
		Los actores están empoderados para entregar el cambio.	0	Aún no están empoderados para ejercer el cambio.
		Los actores están habilitados para operar, usar y mantener el cambio	30	Los actores aún no están habilitados para operar el cambio.
		El cambio es embebido y sostenido	0	Aún no se produce el cambio.

Tabla 15- Nivel de Capacidad Proceso BAI05 Gestionar la introducción del cambio organizativo [83]

2.2.10 BAI09 GESTIONAR LOS ACTIVOS

Descripción del Proceso: "Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia."[84]

Práctica: BAI09.01 Identificar y registrar activos actuales

Descripción: "Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera."[85]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se tienen inventarios de los activos.
- Se controla periódicamente el inventario físico pero no el lógico. Se manejan perfiles y permisos que impiden que los usuarios no autorizados instalen software, pero no se tiene inventario de los programas instalados por equipo.

[83] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[84] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 163
[85] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 164

Práctica: BAI09.02 Gestionar activos críticos

Descripción: “Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.”[86]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene identificados los activos críticos, no se considera el riesgo de falla de los activos críticos ni medidas de reparación o reemplazo en caso de algún daño.
- No se tienen planes de mantenimiento preventivo, en caso de que alguna daño ocurra se planifica aplicar la garantía que ofrecen los proveedores.

Práctica: BAI09.03 Gestionar el ciclo de vida de los activos

Descripción: “Gestionar los activos desde su adquisición hasta su eliminación para asegurar que se utilizan tan eficaz y eficientemente como sea posible y son contabilizados y protegidos físicamente.”[87]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Todos los activos se obtienen teniendo en cuenta solicitudes probadas siguiendo los procesos propios de adquisición del MTOP.
- Los activos son utilizados hasta el final de su vida útil, debido al presupuesto sobretodo, se reasignan los activos.
- Los activos no se eliminan de forma segura, no se tienen procedimientos documentados de lo que debe hacerse al finalizar con el uso de los activos.

[86] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 164
[87] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 165

Práctica: BAI09.04 Optimizar el coste de los activos

Descripción: "Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio."[88]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tienen análisis de costes para optimizar el coste de los activos, una vez adquiridos son utilizados o reutilizados hasta que son obsoletos o se dañan.
- No se hacen análisis de capacidad para identificar activos que no son utilizados al máximo de su capacidad.

Práctica: BAI09.05 Administrar licencias

Descripción: "Administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportarlos requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso."[89]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se adquieren licencias software, se utilizan las que vienen en los activos y se maneja software libre. El resto de licencias comerciales que se utilizan no son originales.

En la Tabla 16- Nivel de Capacidad Proceso BAI09 Gestionar los activos, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**100**	El MTOP tiene un manejo de activos sin documentación, clasificación o etiquetado apropiado.
1 PROCESO EJECUTADO	**El proceso implementado**	**Se alcanzan los siguientes resultados:**	**25**	

[88] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 165
[89] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 166

	cumple con su propósito	Las licencias están alineadas a las necesidades del negocio	0	Las licencias no son originales.
		Los bienes se mantienen en niveles óptimos.	50	Los bienes tienen responsables que se encargan de mantenerlos en buenas condiciones aunque no tienen políticas de uso y mantenimiento de bienes.

Tabla 16- Nivel de Capacidad Proceso BAI09 Gestionar los activos [90]

2.2.11 DSS01 GESTIONAR OPERACIONES

Descripción del Proceso: "Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas."[91]

Práctica: DSS01.01 Ejecutar procedimientos operativos

Descripción: "Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente."[92]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Las actividades se realizan como actividades diarias, no están documentadas ni se tienen controles para asegurar su funcionamiento
- No se tienen actividades operativas programadas.
- No se generan copias de respaldo y no existen políticas tampoco.

Práctica: DSS01.02 Gestionar servicios externalizados de TI

Descripción: "Gestionar la operación de servicios externalizados de TI para mantener la protección de la información empresarial y la confiabilidad de la entrega del servicio."[93]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se evalúa la operación de servicios externalizados de TI.

[90] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[91] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 173
[92] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 174
[93] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 174

Práctica: DSS01.03 Supervisar la infraestructura de TI

Descripción: "Supervisar la infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones."[94]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se almacena información sobre riesgo y rendimiento.
- No se tiene listas de activos a ser monitorizados.
- No se tienen reglas para violaciones de umbral y condiciones de servicio y permitan identificar falsos menores.

Práctica: DSS01.04 Gestionar el entorno

Descripción: "Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno."[95]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se han identificado amenazas ambientales, riesgos, efectos.
- No se han tomado medidas de respaldo, ni para minimizar y mitigar riesgos.

Práctica: DSS01.05 Gestionar las instalaciones

Descripción: "Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo."[96]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Las instalaciones tienen varios controles como seguridad de acceso, señalización, extintores, no existen alfombras, existen salidas de seguridad, sistemas de alimentación ininterrumpida.

---

[94] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 174
[95] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 174
[96] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 175

En la Tabla 17- Nivel de Capacidad Proceso DSS01 Gestionar operaciones, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**0**	Las actividades se realizan como actividades diarias, no están documentadas ni se tienen controles para asegurar su funcionamiento.
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**0**	
		Las actividades operacionales se realizan al ser requeridas y calendarizadas	0	
		Las operaciones son monitorizadas, medidas, reportadas y solucionadas.	0	

Tabla 17- Nivel de Capacidad Proceso DSS01 Gestionar operaciones [97]

2.2.12 DSS04 GESTIONAR LA CONTINUIDAD

Descripción del Proceso: "Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa."[98]

Práctica: DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance

Descripción: "Definir la política y alcance de continuidad de negocio alineada con los objetivos de negocio y de las partes interesadas."[99]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tienen definidos planes ni políticas de continuidad del negocio. El MTOP no reconoce aún la necesidad de tener políticas de continuidad del negocio.

[97] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template
[98] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 185
[99] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 185

Práctica: DSS04.02 Mantener una estrategia de continuidad

Descripción: "Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción."[100]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se han realizado análisis de riesgos, de impacto sobre el negocio, de continuidad frente a fallos o catástrofes, tiempo de recuperación del negocio, interrupción máxima soportable.
- No se han analizado las amenazas que pueden causar pérdidas de continuidad de negocio, análisis de riesgo.

Práctica: DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio

Descripción: "Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas."[101]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene desarrollado un BCP, ni se han definido actividades que aseguren la continuidad.

Práctica: DSS04.04 Ejercitar, probar y revisar el plan de continuidad

Descripción: "Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera."[102]

---

[100] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 187
[101] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 187
[102] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 188

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene desarrollado un BCP, ni se han definido actividades que aseguren la continuidad.

Práctica: DSS04.05 Revisar, mantener y mejorar el plan de continuidad

Descripción: "Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio."[103]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene desarrollado un BCP, ni se han definido actividades que aseguren la continuidad.

Práctica: DSS04.06 Proporcionar formación en el plan de continuidad

Descripción: "Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción."[104]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene desarrollado un BCP, ni se han definido actividades que aseguren la continuidad.

Práctica: DSS04.07 Gestionar acuerdos de respaldo

Descripción: "Mantener la disponibilidad de la información crítica del negocio."[105]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tienen respaldos de información, copias de seguridad del sistema, aplicaciones, datos o documentación ni dentro ni fuera de las instalaciones del MTOP.

---

[103] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 188
[104] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 188
[105] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 189

Práctica: DSS04.08 Ejecutar revisiones post reanudación

Descripción: "Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción."[106]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene desarrollado un BCP, ni se han definido actividades que aseguren la continuidad.

En la Tabla 18- Nivel de Capacidad Proceso DSS04 Gestionar la continuidad, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**100**	No se ha planificado la continuidad del negocio.
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**0**	
		La información crítica del negocio está disponible para el negocio en línea con los niveles mínimos de servicio requeridos.	0	
		Hay suficiente elasticidad para los servicios críticos	0	
		Las pruebas de continuidad de servicio han verificado la efectividad del plan.	0	
		Existe un plan de continuidad actualizado que refleja los requerimientos actuales del negocio	0	
		Las partes internas y externas han sido entrenadas para el plan de continuidad.	0	

Tabla 18- Nivel de Capacidad Proceso DSS04 Gestionar la continuidad[107]

[106] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 189
[107] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template

2.2.13 DSS05 GESTIONAR SERVICIOS DE SEGURIDAD

Descripción del Proceso: "Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad."[108]

Práctica: DSS05.01 Proteger contra software malicioso (malware)

Descripción: "Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura)."[109]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se tienen instalados antivirus actualizados en cada terminal, usando una configuración centralizada, además se tienen controles para impedir el acceso a determinadas páginas.
- No se realizan campañas de concienciación sobre el software malicioso, ni se comunica con el talento humano fuera del área de TI.
- Se filtra el tráfico entrante.

Práctica: DSS05.02 Gestionar la seguridad de la red y las conexiones

Descripción: "Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión."[110]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- La red de la empresa se encuentra protegida por firewall y también se tienen restricciones de acceso, autentificación, políticas no documentadas de control de tráfico entrante y saliente.

---

[108] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 191
[109] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 192
[110] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 193

Práctica: DSS05.03 Gestionar la seguridad de los puestos de usuario final

Descripción: "Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida."[111]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Los puestos de usuario final están protegidos con antivirus y mecanismos de autentificación para el dispositivo y acceso a la red.
- No existe una correcta forma de eliminación de activos.

Práctica: DSS05.04 Gestionar la identidad del usuario y el acceso lógico

Descripción: "Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio."[112]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se manejan perfiles y roles de usuario, y de acuerdo a su clasificación tienen más permisos o restricciones.
- No se tienen procedimientos para administrar los cambios de derecho de acceso, creación, modificación y eliminación, se hace de acuerdo a la necesidad.

Práctica: DSS05.05 Gestionar el acceso físico a los activos de TI

Descripción: "Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las

[111] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 193
[112] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 194

personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte."[113]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se tienen seguridades de acceso para las instalaciones y se deben realizar peticiones o tener un rol apropiado para ingresar a los lugares restringidos, por ejemplo la sala de servidores.
- No se actualizan los perfiles de acceso periódicamente sino bajo necesidad.
- Se registran todos los puntos de entrada y accesos a las ubicaciones de TI. Todo el personal debe tener su identificación visible en todo momento.

Práctica: DSS05.06 Gestionar documentos sensibles y dispositivos de salida

Descripción: "Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad."[114]

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- No se tiene clasificación de documentos sensibles, etiquetado, medidas de seguridad para la divulgación o no divulgación de la información. No existen controles para dispositivos de salida.

Práctica: DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Descripción: "Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes."[115]

---

[113] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 194
[114] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 195
[115] Fuente: Tomado de COBIT 5 Enabling Spanish, pág. 195

Del análisis de esta práctica se obtuvieron los siguientes resultados:

- Se registran los eventos relacionados a seguridad, se tienen herramientas para monitorizar la seguridad de la infraestructura.
- No se tienen procedimientos de recopilación de evidencias.

En la Tabla 19- Nivel de Capacidad Proceso DSS05 Gestionar servicios de seguridad, se realiza el análisis del nivel de capacidad del proceso.

Nivel de capacidad	Atributo	Criterio	Cump%	Observaciones
0 PROCESO INCOMPLETO	**El proceso no se ha implementado, o falla para alcanzar el objetivo del proceso**	**En este nivel, hay poca o no hay evidencia del alcance del propósito de este proceso.**	**100**	No se gestiona la seguridad sin embargo se tienen medidas de seguridad implementadas.
1 PROCESO EJECUTADO	**El proceso implementado cumple con su propósito**	**Se alcanzan los siguientes resultados:**	**40**	
		La seguridad de las redes y comunicaciones cumple con las necesidades del negocio.	50	
		La información procesada, almacenada y transmitida por terminales está protegida.	50	
		Todos los usuarios son identificados y tienen derecho de acceso de acuerdo con su rol de negocio.	50	
		Se han tomado medidas físicas para proteger la información de acceso no autorizado, daño e interferencia al momento de procesar, almacenar o transmitir	50	
		La información electrónica está asegurada apropiadamente al ser almacenada, transmitida o destruida	0	

Tabla 19- Nivel de Capacidad Proceso DSS05 Gestionar servicios de seguridad[116]

[116] Fuente: Tabla generada por la autora en base a la herramienta Self Assesment Template

CAPÍTULO III: RESULTADOS DE LA AUDITORÍA

3.1 ANÁLISIS DE RESULTADOS

El primer paso para la realización de la Auditoría fue la selección de los procesos para analizar, esta decisión se tomó conjuntamente con el comité informático. Se trabajó con 13 procesos y 4 dominios, los mismos que se listan a continuación:

EVALUAR, ORIENTAR Y SUPERVISAR (EMD)

- EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno
- EDM03 Asegurar la optimización del riesgo
- EDM04 Asegurar la optimización de recursos

ALINEAR, PLANEAR Y ORGANIZAR (APO)

- APO01 Gestionar el marco de gestión de TI
- APO02 Gestionar la estrategia
- APO07 Gestionar los recursos humanos
- AP012 Gestionar el riesgo
- AP013 Gestionar la seguridad

CONSTRUIR, ADQUIRIR E IMPLEMENTAR (BAI):

- BAI05 Gestionar la introducción del cambio organizativo
- BAI09 Gestionar los activos

ENTREGAR, DAR SERVICIO Y SOPORTE (DSS):

- DSS01 Gestionar operaciones
- DSS04 Gestionar la continuidad
- DSS05 Gestionar servicios de seguridad

El dominio que Supervisar, Evaluar y Valorar no ha sido tomado en cuenta dentro de la selección ya que todavía no existen muchos controles

implementados por la Unidad Informática, así que se le dio más importancia a los procesos que van a permitir establecer las bases para un Gobierno de TI estable dentro de la empresa.

Una vez realizada la Auditoría se analizó el nivel de capacidad de los procesos seleccionados, se obtuvieron los siguientes resultados:

PROCESO	Nivel de Capacidad
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	0
EDM03 Asegurar la optimización del riesgo	0
EDM04 Asegurar la optimización de recursos	2
APO01 Gestionar el marco de gestión de TI	1
APO02 Gestionar la estrategia	0
APO07 Gestionar los recursos humanos	0
AP012 Gestionar el riesgo	0
AP013 Gestionar la seguridad	0
BAI05 Gestionar la introducción del cambio organizativo	1
BAI09 Gestionar los activos	1
DSS01 Gestionar operaciones	0
DSS04 Gestionar la continuidad	0
DSS05 Gestionar servicios de seguridad	0

Tabla 17- Nivel de capacidad de los procesos en el MTOP[117]

Como se puede apreciar en la tabla 17 – Nivel de capacidad de los procesos en el MTOP, la mayor parte de los procesos están en un nivel 0, tres procesos tienen un nivel 1 y sólo un proceso tiene un nivel 2.

Los procesos de nivel 0, Proceso incompleto, están incompletos, no están implementados o se tienen nociones básicas pero no se logra ningún objetivo.

Los procesos de nivel 1, Proceso ejecutado, son procesos ya implementados que alcanzan su objetivo.

Los procesos de nivel 2, Proceso Gestionado, son procesos que ya están implementados, alcanzan su objetivo y también están gestionados, existe una planificación, supervisión y ajuste, además los resultados son establecidos, controlados y mantenidos.

[117] Fuente: tabla generada por la Autora

A continuación se detallan el Informe Preliminar, el Informe Técnico y el Informe Ejecutivo. El Informe Técnico y Ejecutivo están dirigidos al Ing. Dirney Escobar como director de Tecnologías de la Información del Ministerio de Transporte y Obras Públicas.

Los informes comparten las conclusiones y recomendaciones de esta auditoría.

3.2 INFORME PRELIMINAR

El objetivo del presente informe es detallar los pasos realizados en la Auditoría al Sistema Informático del Ministerio de Transporte y Obras Públicas.

En el Capítulo I se realizó:

- Planteamiento del Problema
- Caracterización del Ministerio
- Caracterización de la Unidad informática
- Planteamiento de la metodología usando COBIT 5

En el capítulo II se realizó:

- Planificación de la Auditoría
- Selección de los procesos para la auditoría
- Ejecución de la Auditoría

En el Capítulo III se detallan:

- Resultados de la Auditoría
- Informe Técnico
- Informe Ejecutivo

El presente trabajo está a disposición de ejecutivos y el personal involucrado.

3.3 INFORME TÉCNICO

Este informe contiene resultados obtenidos en la Auditoría del Sistema Informático del Ministerio de Transporte y Obras Públicas.

Se utilizó el marco de trabajo COBIT 5, se seleccionaron 13 de los 37 procesos existentes para analizar en el MTOP, a continuación la lista de los procesos analizados:

Evaluar, Dirigir y Monitorear (EDM)

- EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno
- EDM03 Asegurar la optimización del riesgo
- EDM04 Asegurar la optimización de recursos

Alinear, Planear y Organizar (APO)

- APO01 Gestionar el marco de gestión de TI
- APO02 Gestionar la estrategia
- APO07 Gestionar los recursos humanos
- AP012 Gestionar el riesgo
- AP013 Gestionar la seguridad

Construir, Adquirir e Implementar (BAI)

- BAI05 Gestionar la introducción del cambio organizativo
- BAI09 Gestionar los activos

Entregar, dar Servicio y Soporte (DSS)

- DSS01 Gestionar operaciones
- DSS04 Gestionar la continuidad
- DSS05 Gestionar servicios de seguridad

Los siguientes resultados fueron obtenidos mediante el análisis de los procesos:

PROCESO	Nivel de Capacidad
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	0
EDM03 Asegurar la optimización del riesgo	0
EDM04 Asegurar la optimización de recursos	2
APO01 Gestionar el marco de gestión de TI	1
APO02 Gestionar la estrategia	0
APO07 Gestionar los recursos humanos	0
AP012 Gestionar el riesgo	0
AP013 Gestionar la seguridad	0
BAI05 Gestionar la introducción del cambio organizativo	1
BAI09 Gestionar los activos	1
DSS01 Gestionar operaciones	0
DSS04 Gestionar la continuidad	0
DSS05 Gestionar servicios de seguridad	0

Nivel de capacidad de los procesos seleccionados

Los niveles de capacidad se evalúan de la siguiente forma:

Nivel de capacidad	Descripción
Nivel 0 – Proceso incompleto	El proceso no está implementado o en su defecto no alcanza su objetivo. No existe ninguna evidencia de ningún logro del proceso.
Nivel 1 – Proceso ejecutado	El proceso alcanza su propósito. (1 atributo)
Nivel 2 – Proceso gestionado	El proceso ya está implementado y gestionado (planificado, supervisado y ajustado). Los resultados están establecidos, controlados y mantenidos. (2 atributos)
Nivel 3 – Proceso establecido	El proceso gestionado está implementado usando un proceso definido que permite alcanzar sus resultados de proceso. (2 atributos)
Nivel 4 – Proceso predecible	El proceso establecido antes se ejecuta dentro de los límites definidos y permite alcanzar los resultados de proceso. (2 atributos)
Nivel 5 – Proceso optimizado	El proceso predecible es mejorado continuamente para cumplir con las metas empresariales. (2 atributos)

PROCESOS

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

Nivel: 0

Conclusiones:

El sistema de gobierno de la Unidad Informática tiene que ser establecido, se tienen normas y obligaciones que deben ser establecidas, sin embargo, no se tiene el completo apoyo de parte de las autoridades.

Recomendaciones:

Se recomienda conversar con la alta gerencia para que entienda la importancia que debe tener la Unidad Informática en cada empresa.

Empezar a alinear las necesidades de todo el ministerio con las de la Unidad Informática, de esta forma se pueden elaborar planes permitan que la Unidad Informática esté alineada con el negocio.

EDM03 Asegurar la optimización del riesgo

Nivel: 0

Conclusiones:

El MTOP no tiene un análisis de riesgo y no se gestionan los riesgos de ninguna forma, se tienen actividades que se hacen para controlar y mitigar el riesgo pero no son formales ni están documentadas

Recomendaciones:

Es fundamental que se realice un Análisis de Riesgo que incluya la probabilidad de ocurrencia e impacto en caso de que ocurra. Se debe contemplar la situación actual y a futuro.

Elaborar un plan de riesgos, además analizar el apetito de riesgo y analizar acciones que se pueden tomar para mitigar los riesgos teniendo en cuenta el presupuesto.

EDM04 Asegurar la optimización de recursos

Nivel: 2

Conclusiones:

Se realizan inventarios, proyecciones y análisis de crecimiento a futuro en conjunto con talento humano sin embargo no se tienen políticas para el cuidado de los equipos de los usuarios finales.

Recomendaciones:

Generar y comunicar políticas para que los usuarios tengan un buen manejo de sus equipos y éstos puedan funcionar correctamente optimizando su ciclo de vida.

Capacitar a los usuarios finales en todo el ministerio del correcto uso de los recursos.

Analizar las tendencias futuras para tomar decisiones informadas y teniendo en cuenta la asignación del presupuesto.

APO01 Gestionar el marco de gestión de TI

Nivel: 1

Conclusiones:

Se ha creado un comité de 3 personas para generar el marco de gestión de TI, sin embargo sus reuniones son escasas debido a la gran cantidad de actividades que deben cumplir.

Recomendaciones:

Socializar a los empleados estos planes para obtener el apoyo del elemento humano, asignar roles y responsabilidades.

APO02 Gestionar la estrategia

Nivel: 0

Conclusiones:

Se reconoce la necesidad de una estrategia de TI, sin embargo aún no se ha desarrollado o implementado una.

Recomendaciones:

Trabajar en torno a las necesidades de la empresa para estar alineados a ella y satisfacer sus necesidades. Realizar un análisis de diferencias para entender mejor en donde estamos y a donde queremos llegar.

APO07 Gestionar los recursos humanos

Nivel: 0

Conclusiones:

La Unidad Informática no tiene el apoyo deseado al momento de contratar personal y sienten que las actividades que realizan son muchas para el personal.

No existe ningún procedimiento de capacitación para los nuevos empleados, se capacitan conforme a las actividades que van realizando.

No existe tampoco documentación sobre las actividades que realizan los empleados y los procedimientos que siguen, por tanto se vuelven indispensables para el ministerio.

Recomendaciones:

Elaborar un plan de capacitación para los empleados.

Documentar las actividades y procedimientos que realizan los empleados así nadie se vuelve indispensable.

AP012 Gestionar el riesgo

Nivel: 0

Conclusiones:

El MTOP reconoce la necesidad de gestionar el riesgo, sin embargo no se tiene elaborado un plan de gestión de riesgo

El MTOP no gestiona el riesgo, no mantiene un método de obtención de información ni clasificación de datos referente a los riesgos. No se tiene ningún análisis de riesgo.

Recomendaciones:

Realizar análisis de riesgo y establecer formas de obtener datos para procesarlos y obtener información útil.

Generar un plan de gestión de riesgos con información útil y actualizada, se debe incluir los atributos de riesgo, frecuencia, impacto, respuesta. En el plan además se deben detallar las medidas efectivas para responder a los riegos.

AP013 Gestionar la seguridad

El MTOP reconoce la necesidad de gestionar la seguridad, aunque no hay plan de seguridad, pero se realizan procedimientos de seguridad del día a día, por ejemplo:

- Seguridad Física: En lo que refiere a seguridad física, existe un personal de guardia privada en la entrada del edificio, el mismo que verifica que no se ingrese material potencialmente inseguro, así como verificar quien ingresa y cuál es su propósito dentro de las instalaciones, en el octavo piso donde se encuentra la Unidad de Información existe otro guardia que cuida la entrada a la unidad de información. La seguridad de la unidad de información consiste en una puerta que solo se abre un una tarjeta magnética o identificarse con el guardia. La puerta siempre está cerrada. Dentro de las instalaciones existen extintores en caso de incendios y tienen planes de escape en una posible emergencia. En lo que se refiere a los servidores, el personal no interactúa directamente con ellos sino que lo hace desde conexiones remotas, los servidores se encuentran es salas frías, esta sala está a cargo del personal autorizado.
- Seguridad lógica: Existen perfiles de usuario y contraseñas para el personal autorizado encargado de algún servidor. No existen políticas para el manejo de contraseñas.
- Seguridad legal: Las licencias de software que manejan los ordenadores no son originales, sólo las de los sistemas operativos vienen instaladas de fábrica.
- Seguridad de datos: El MTOP no tiene planes de contingencia, respaldo sino que toda la información se almacena en los servidores localizados en este mismo edificio.

Recomendaciones:

Realizar un análisis de riesgo de la seguridad de la información. Crear un Sistema de Gestión de Seguridad de la Información, establecer controles y medidas para mitigar el riesgo.

Comunicar el plan a todo el personal del ministerio.

BAI05 Gestionar la introducción del cambio organizativo

Nivel: 0

Conclusiones:

El MTOP está en un proceso de cambio organizativo debido a las leyes y normas estatales que deben cumplirse, se tiene clara la necesidad del cambio y se ha conformado un equipo para lograr la transición, sin embargo el equipo tiene problemas para reunirse debido a la gran cantidad de actividades del personal.

El deseo de cambio ha sido entendido pero aún no se tiene todo el apoyo para producirse, es necesario que el personal entienda el cambio.

Recomendaciones:

Comunicar al personal la necesidad del cambio, es necesario que sean partes activas para poder minimizar la resistencia al cambio, sobre todo buscar a los líderes para que ellos faciliten la transición.

BAI09 Gestionar los activos

Nivel: 1

Conclusiones:

Se tiene un inventario de activos, se han asignado a responsables pero no se tienen políticas de mantenimiento de los activos para los usuarios finales, no se tienen mantenimientos preventivos. No se controla el inventario lógico.

No se tienen licencias originales, exceptuando las de los sistemas operativos que vienen instaladas en los equipos comprados. Los servidores utilizan software libre.

Recomendaciones:

Cambiar el software sin licencias originales a software libre.

Generar un manual de mantenimiento de los activos para que los usuarios finales puedan utilizarlos de una mejor manera y de esta forma se optimice el ciclo de vida de los activos.

Seleccionar los activos críticos.

Analizar el porcentaje del uso de los activos, de esta forma se puede evitar que los activos sean subutilizados y tener en cuenta el costo de los activos para realizar compras informadas.

DSS01 Gestionar operaciones

Nivel: 1

Conclusiones:

Las instalaciones tienen varios controles como seguridad de acceso, señalización, extintores, no existen alfombras, existen salidas de seguridad, sistemas de alimentación ininterrumpida.

Las actividades se realizan como actividades diarias, no están documentadas ni se tienen controles para asegurar su funcionamiento, además no se tienen actividades operativas programadas.

No se generan copias de respaldo y no existen políticas tampoco. No se tiene listas de activos a ser monitorizados, no se tienen reglas para violaciones de umbral y condiciones de servicio y permitan identificar falsos menores.

Recomendaciones:

Documentar los controles que se tienen, generar copiar y políticas de respaldo de la información y también establecer controles para mantener los respaldos actualizados, completos, íntegros y seguros, impidiendo que cualquier persona tenga acceso a información clasificada respaldada.

Crear una lista de activos para ser monitorizados, establecer reglas para violaciones de umbrales lo que permita identificar falsos menores.

DSS04 Gestionar la continuidad

Nivel: 0

Conclusiones:

No se tiene un plan para gestionar la continuidad, ni se ha planteado alguna actividad para gestionar la continuidad.

Recomendaciones:

Crear un plan para gestionar la continuidad, por ejemplo un plan de continuidad del negocio, BCP, que incluya las prácticas para restaurar las actividades críticas frente a un desastre o una interrupción de las actividades.

Analizar los posibles escenarios que pueden producirse que obliguen a interrumpir las actividades de la Unidad Informática y proponer una serie de actividades que permitan recuperar la funcionalidad en el menor tiempo posible.

DSS05 Gestionar servicios de seguridad

Nivel: 1

Conclusiones:

Se toman medidas de seguridad como mantener antivirus actualizados en cada terminal, autentificación, filtrado de tráfico en la red, uso de firewall, manejo de roles y perfiles de acceso, además se gestiona el acceso tanto físico como lógico.

No se documentan las medidas de seguridad que se toman, las actividades se realizan de acuerdo a la necesidad. No se tiene un correcto uso de la información fuera del sistema informático, por ejemplo la información sensible no se encuentra debidamente etiquetada ni tiene un correcto proceso de eliminación.

Recomendaciones:

Documentar las medidas de seguridad que se toman, establecer controles para monitorear las medidas de seguridad que se ejecutan en la Unidad Informática para determinar si son eficientes, en caso de que no lo sean buscar nuevas alternativas que ofrezcan mejores soluciones.

3.4 INFORME EJECUTIVO.

OBJETIVO: Este informe pretende informar de los resultados obtenidos en la Auditoría del Sistema Informático del Ministerio de Transporte y Obras Públicas, usando una metodología basada en COBIT 5.

Se utilizó el marco de trabajo COBIT 5, del cual se seleccionaron 13 de los 37 procesos existentes para analizar en el MTOP, a continuación la lista de los procesos analizados:

Evaluar, Dirigir y Monitorear (EDM)

- EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno
- EDM03 Asegurar la optimización del riesgo
- EDM04 Asegurar la optimización de recursos

Alinear, Planear y Organizar (APO)

- APO01 Gestionar el marco de gestión de TI
- APO02 Gestionar la estrategia
- APO07 Gestionar los recursos humanos
- AP012 Gestionar el riesgo
- AP013 Gestionar la seguridad

Construir, Adquirir e Implementar (BAI)

- BAI05 Gestionar la introducción del cambio organizativo
- BAI09 Gestionar los activos

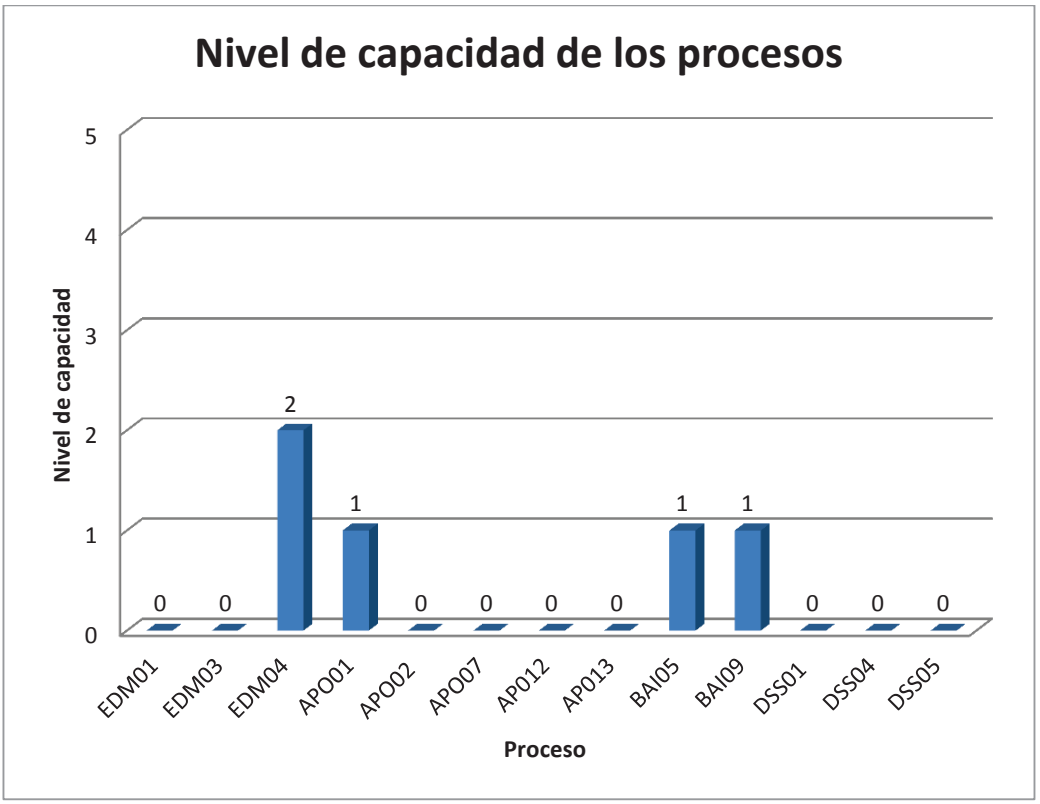
Entregar, dar Servicio y Soporte (DSS)

- DSS01 Gestionar operaciones
- DSS04 Gestionar la continuidad
- DSS05 Gestionar servicios de seguridad

Los resultados que se obtuvieron con la Auditoría se muestran a continuación:

PROCESO	Nivel de Capacidad
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	0
EDM03 Asegurar la optimización del riesgo	0
EDM04 Asegurar la optimización de recursos	2
APO01 Gestionar el marco de gestión de TI	1
APO02 Gestionar la estrategia	0
APO07 Gestionar los recursos humanos	0
AP012 Gestionar el riesgo	0
AP013 Gestionar la seguridad	0
BAI05 Gestionar la introducción del cambio organizativo	1
BAI09 Gestionar los activos	1
DSS01 Gestionar operaciones	0
DSS04 Gestionar la continuidad	0
DSS05 Gestionar servicios de seguridad	0

Nivel de capacidad de los procesos



Nivel de capacidad de los procesos seleccionados

Los niveles de capacidad se evalúan de la siguiente forma:

Nivel de capacidad	Descripción
Nivel 0 – Proceso incompleto	El proceso no está implementado o en su defecto no alcanza su objetivo. No existe ninguna evidencia de ningún logro del proceso.
Nivel 1 – Proceso ejecutado	El proceso alcanza su propósito. (1 atributo)
Nivel 2 – Proceso gestionado	El proceso ya está implementado y gestionado (planificado, supervisado y ajustado). Los resultados están establecidos, controlados y mantenidos. (2 atributos)
Nivel 3 – Proceso establecido	El proceso gestionado está implementado usando un proceso definido que permite alcanzar sus resultados de proceso. (2 atributos)
Nivel 4 – Proceso predecible	El proceso establecido antes se ejecuta dentro de los límites definidos y permite alcanzar los resultados de proceso. (2 atributos)
Nivel 5 – Proceso optimizado	El proceso predecible es mejorado continuamente para cumplir con las metas empresariales. (2 atributos)

CONCLUSIONES Y RECOMENDACIONES:

Las conclusiones y recomendaciones son las mismas que las del informe técnico:

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

Nivel: 0

Conclusiones:

El sistema de gobierno de la Unidad Informática tiene que ser establecido, se tienen normas y obligaciones que deben ser establecidas, sin embargo, no se tiene el completo apoyo de parte de las autoridades.

Recomendaciones:

Se recomienda conversar con la alta gerencia para que entienda la importancia que debe tener la Unidad Informática en cada empresa.

Empezar a alinear las necesidades de todo el ministerio con las de la Unidad Informática, de esta forma se pueden elaborar planes permitan que la Unidad Informática esté alineada con el negocio.

EDM03 Asegurar la optimización del riesgo

Nivel: 0

Conclusiones:

El MTOP no tiene un análisis de riesgo y no se gestionan los riesgos de ninguna forma, se tienen actividades que se hacen para controlar y mitigar el riesgo pero no son formales ni están documentadas

Recomendaciones:

Es fundamental que se realice un Análisis de Riesgo que incluya la probabilidad de ocurrencia e impacto en caso de que ocurra. Se debe contemplar la situación actual y a futuro.

Elaborar un plan de riesgos, además analizar el apetito de riesgo y analizar acciones que se pueden tomar para mitigar los riesgos teniendo en cuenta el presupuesto.

EDM04 Asegurar la optimización de recursos

Nivel: 2

Conclusiones:

Se realizan inventarios, proyecciones y análisis de crecimiento a futuro en conjunto con talento humano sin embargo no se tienen políticas para el cuidado de los equipos de los usuarios finales.

Recomendaciones:

Generar y comunicar políticas para que los usuarios tengan un buen manejo de sus equipos y éstos puedan funcionar correctamente optimizando su ciclo de vida.

Capacitar a los usuarios finales en todo el ministerio del correcto uso de los recursos.

Analizar las tendencias futuras para tomar decisiones informadas y teniendo en cuenta la asignación del presupuesto.

APO01 Gestionar el marco de gestión de TI

Nivel: 1

Conclusiones:

Se ha creado un comité de 3 personas para generar el marco de gestión de TI, sin embargo sus reuniones son escasas debido a la gran cantidad de actividades que deben cumplir.

Recomendaciones:

Socializar a los empleados estos planes para obtener el apoyo del elemento humano, asignar roles y responsabilidades.

APO02 Gestionar la estrategia

Nivel: 0

Conclusiones:

Se reconoce la necesidad de una estrategia de TI, sin embargo aún no se ha desarrollado o implementado una.

Recomendaciones:

Trabajar en torno a las necesidades de la empresa para estar alineados a ella y satisfacer sus necesidades. Realizar un análisis de diferencias para entender mejor en donde estamos y a donde queremos llegar.

APO07 Gestionar los recursos humanos

Nivel: 0

Conclusiones:

La Unidad Informática no tiene el apoyo deseado al momento de contratar personal y sienten que las actividades que realizan son muchas para el personal.

No existe ningún procedimiento de capacitación para los nuevos empleados, se capacitan conforme a las actividades que van realizando.

No existe tampoco documentación sobre las actividades que realizan los empleados y los procedimientos que siguen, por tanto se vuelven indispensables para el ministerio.

Recomendaciones:

Elaborar un plan de capacitación para los empleados.

Documentar las actividades y procedimientos que realizan los empleados así nadie se vuelve indispensable.

AP012 Gestionar el riesgo

Nivel: 0

Conclusiones:

El MTOP reconoce la necesidad de gestionar el riesgo, sin embargo no se tiene elaborado un plan de gestión de riesgo

El MTOP no gestiona el riesgo, no mantiene un método de obtención de información ni clasificación de datos referente a los riesgos. No se tiene ningún análisis de riesgo.

Recomendaciones:

Realizar análisis de riesgo y establecer formas de obtener datos para procesarlos y obtener información útil.

Generar un plan de gestión de riesgos con información útil y actualizada, se debe incluir los atributos de riesgo, frecuencia, impacto, respuesta. En el plan además se deben detallar las medidas efectivas para responder a los riegos.

AP013 Gestionar la seguridad

El MTOP reconoce la necesidad de gestionar la seguridad, aunque no hay plan de seguridad, pero se realizan procedimientos de seguridad del día a día, por ejemplo:

- Seguridad Física: En lo que refiere a seguridad física, existe un personal de guardia privada en la entrada del edificio, el mismo que verifica que no se ingrese material potencialmente inseguro, así como verificar quien ingresa y cuál es su propósito dentro de las instalaciones, en el octavo piso donde se encuentra la Unidad de Información existe otro guardia que cuida la entrada a la unidad de información. La seguridad de la unidad de información consiste en una puerta que solo se abre un una tarjeta magnética o identificarse con el guardia. La puerta siempre está cerrada. Dentro de las instalaciones existen extintores en caso de

incendios y tienen planes de escape en una posible emergencia. En lo que se refiere a los servidores, el personal no interactúa directamente con ellos sino que lo hace desde conexiones remotas, los servidores se encuentran es salas frías, esta sala está a cargo del personal autorizado.

- Seguridad lógica: Existen perfiles de usuario y contraseñas para el personal autorizado encargado de algún servidor. No existen políticas para el manejo de contraseñas.
- Seguridad legal: Las licencias de software que manejan los ordenadores no son originales, sólo las de los sistemas operativos vienen instaladas de fábrica.
- Seguridad de datos: El MTOP no tiene planes de contingencia, respaldo sino que toda la información se almacena en los servidores localizados en este mismo edificio.

Recomendaciones:

Realizar un análisis de riesgo de la seguridad de la información. Crear un Sistema de Gestión de Seguridad de la Información, establecer controles y medidas para mitigar el riesgo.

Comunicar el plan a todo el personal del ministerio.

BAI05 Gestionar la introducción del cambio organizativo

Nivel: 0

Conclusiones:

El MTOP está en un proceso de cambio organizativo debido a las leyes y normas estatales que deben cumplirse, se tiene clara la necesidad del cambio y se ha conformado un equipo para lograr la transición, sin embargo el equipo tiene problemas para reunirse debido a la gran cantidad de actividades del personal.

El deseo de cambio ha sido entendido pero aún no se tiene todo el apoyo para producirse, es necesario que el personal entienda el cambio.

Recomendaciones:

Comunicar al personal la necesidad del cambio, es necesario que sean partes activas para poder minimizar la resistencia al cambio, sobre todo buscar a los líderes para que ellos faciliten la transición.

BAI09 Gestionar los activos

Nivel: 1

Conclusiones:

Se tiene un inventario de activos, se han asignado a responsables pero no se tienen políticas de mantenimiento de los activos para los usuarios finales, no se tienen mantenimientos preventivos. No se controla el inventario lógico.

No se tienen licencias originales, exceptuando las de los sistemas operativos que vienen instaladas en los equipos comprados. Los servidores utilizan software libre.

Recomendaciones:

Cambiar el software sin licencias originales a software libre.

Generar un manual de mantenimiento de los activos para que los usuarios finales puedan utilizarlos de una mejor manera y de esta forma se optimice el ciclo de vida de los activos.

Seleccionar los activos críticos.

Analizar el porcentaje del uso de los activos, de esta forma se puede evitar que los activos sean subutilizados y tener en cuenta el costo de los activos para realizar compras informadas.

DSS01 Gestionar operaciones

Nivel: 1

Conclusiones:

Las instalaciones tienen varios controles como seguridad de acceso, señalización, extintores, no existen alfombras, existen salidas de seguridad, sistemas de alimentación ininterrumpida.

Las actividades se realizan como actividades diarias, no están documentadas ni se tienen controles para asegurar su funcionamiento, además no se tienen actividades operativas programadas.
No se generan copias de respaldo y no existen políticas tampoco. No se tiene listas de activos a ser monitorizados, no se tienen reglas para violaciones de umbral y condiciones de servicio y permitan identificar falsos menores.

Recomendaciones:
Documentar los controles que se tienen, generar copiar y políticas de respaldo de la información y también establecer controles para mantener los respaldos actualizados, completos, íntegros y seguros, impidiendo que cualquier persona tenga acceso a información clasificada respaldada.
Crear una lista de activos para ser monitorizados, establecer reglas para violaciones de umbrales lo que permita identificar falsos menores.

DSS04 Gestionar la continuidad
Nivel: 0
Conclusiones:
No se tiene un plan para gestionar la continuidad, ni se ha planteado alguna actividad para gestionar la continuidad.

Recomendaciones:
Crear un plan para gestionar la continuidad, por ejemplo un plan de continuidad del negocio, BCP, que incluya las prácticas para restaurar las actividades críticas frente a un desastre o una interrupción de las actividades.
Analizar los posibles escenarios que pueden producirse que obliguen a interrumpir las actividades de la Unidad Informática y proponer una serie de actividades que permitan recuperar la funcionalidad en el menor tiempo posible.

DSS05 Gestionar servicios de seguridad

Nivel: 1

Conclusiones:

Se toman medidas de seguridad como mantener antivirus actualizados en cada terminal, autentificación, filtrado de tráfico en la red, uso de firewall, manejo de roles y perfiles de acceso, además se gestiona el acceso tanto físico como lógico.

No se documentan las medidas de seguridad que se toman, las actividades se realizan de acuerdo a la necesidad. No se tiene un correcto uso de la información fuera del sistema informático, por ejemplo la información sensible no se encuentra debidamente etiquetada ni tiene un correcto proceso de eliminación.

Recomendaciones:

Documentar las medidas de seguridad que se toman, establecer controles para monitorear las medidas de seguridad que se ejecutan en la Unidad Informática para determinar si son eficientes, en caso de que no lo sean buscar nuevas alternativas que ofrezcan mejores soluciones.

CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

El nivel de decisión de la Unidad Informática es un nivel inadecuado, las autoridades aún necesitan entender la importancia que ésta tiene en la actualidad y los beneficios que puede aportar.

La mayor parte de los procesos evaluados están en un nivel de capacidad 0, lo ideal sería implementar los procesos pero también gestionarlos para llegar a un nivel de capacidad 2.

Se necesita el apoyo de la gerencia para poder llevar a cabo el cambio que las autoridades se han planteado, por lo tanto es fundamental que las autoridades entiendan la importancia que tiene la Unidad Informática en la actualidad y los beneficios de una buena gestión.

No sólo tienen que cambiarse la forma en la que el Ministerio ve a la tecnología, sino la forma en la que se maneja la información y se administran los procesos, por ejemplo, aún sigue existiendo personal que es indispensable debido a que sus actividades y conocimientos no están documentados y son expertos en el tema.

Las empresas públicas en el país tienen que apegarse a estas mismas normas, por lo tanto este análisis sobre el Sistema Informático del MTOP puede ser útil para otras empresas públicas que estén pasando por el mismo proceso.

4.2 RECOMENDACIONES

Buscar oportunidades de diálogo con las personas que están encargadas de la dirección de la institución, en este caso con la Ministra. Para poder realizar un cambio efectivo es necesario el apoyo de la alta gerencia.

Trabajar con los líderes de cada departamento o área para que no se resistan al cambio sino que puedan aportar, también deben recibir una charla para entender la importancia de la Unidad Informática en la actualidad.

Capacitar a todo el personal del Ministerio y comunicar las políticas que deben ser implantadas, el cambio no sólo se da dentro del área informática, sino en todo el ministerio.

Aunque el presupuesto sea limitado, existen varios controles que se pueden empezar a aplicar y es prioritario que se generen los diferentes planes que son fundamentales para el correcto funcionamiento de la Unidad Informática, por ejemplo: el plan de contingencia, plan de capacitación, plan operativo, plan de recuperación de desastres, entre otros.

BIBLIOGRAFÍA

- ISACA. (05 de 10 de 2012). *COBIT5-Enabling-Spanish* de ISACA: www.isaca.org/COBIT/Documents/COBIT5-Enabling-Spanish.pdf
- ISACA. (05 de 10 de 2012). *COBIT5-Spanish.* de ISACA: www.isaca.org/COBIT/Documents/COBIT5- Spanish.pdf
- J.E.M.V Pablo Andrés Cilio Muñoz, EVALUACIÓN Y PLAN DE MEJORA CASABACA, Escuela Politécnica Nacional. Quito, 2012
- H. Enrique, Auditoria en Informática, 2da Edición, México: McGraw - Hill, 2001
- ECHENIQUE, García José Antonio. “Auditoría en Informática”, McGraw – Hill. España. 1990.

ANEXOS

ANEXO 1:

ESTATUTO ORGANICO DE GESTION ORGANIZACIONAL POR PROCESOS

14. Agenda de recorridos de seguimiento de avance de los proyectos con los delegados de las entidades crediticias para evaluar avance de proyectos e informes de resultados.
15. Inventario actualizado de los proyectos que se financian con recursos de créditos internos y externos.
16. Presentaciones informativas y de avances de proyectos financiados con los diferentes programas de crédito.
17. Solicitudes de desembolsos.
18. Solicitudes de ampliación de plazo para primer y último desembolsos.

3.2.1.6 DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

a. MISIÓN.- Administrar y proveer servicios informáticos y tecnologías de la información y comunicaciones para el procesamiento de datos y acceso a la información, garantizando la disponibilidad, integridad y confiabilidad de la información.

Responsable: Director Técnico de Área

b. Atribuciones y Responsabilidades:

1. Formular el Plan Estratégico;
2. Proponer el Plan Anual de Inversiones de la Unidad;
3. Identificar las necesidades del Ministerio de Transporte y Obras Públicas referentes a la gestión tecnológica;
4. Aprobar los inventarios tecnológicos del Ministerio de Transporte y Obras Públicas;
5. Participar en la elaboración de los informes técnicos dentro del proceso de adquisición de hardware, software, conectividad y/o herramientas de diseño y desarrollo de aplicaciones informáticas;
6. Administrar y monitorear el uso de recursos tecnológicos de que dispone el Ministerio de Transporte y Obras Públicas: hardware, software y comunicaciones;
7. Gestionar soluciones informáticas de hardware, software y comunicaciones;
8. Gestionar los servicios de mantenimiento y reparación de la infraestructura tecnológica y de apoyo;
9. Proponer los términos de referencia y pliegos de contratación concernientes a la contratación de las tecnologías de información y comunicaciones;
10. Coordinar con la Dirección de Administración de Recursos Humanos, la capacitación en el área de las tecnologías de información y comunicaciones de los funcionarios, servidores y trabajadores de todas las unidades del Ministerio de Transporte y Obras Públicas a nivel nacional;
11. Establecer directrices para la seguridad física del equipo informático, su correcto uso y mantenimiento; y,
12. Proponer la adquisición y contratación de servicios relacionados con las tecnologías de información y comunicaciones en base a los términos de referencia y especificaciones técnicas desarrollados por la Unidad.

La Dirección de Tecnologías de la Información y Comunicaciones tiene una estructura conformada por equipos técnicos de trabajo y para el cumplimiento de su Misión contará con las siguientes unidades: Planificación y Seguridad Informática, Base de Datos, Aplicaciones y Soporte Técnico.

3.2.1.6.1 Planificación y Seguridad Informática

Planificación

a. Productos y Servicios

1. Plan Operativo Anual de la Dirección.
2. Informes semestrales de evaluación del Plan Operativo Anual.
3. Procedimientos técnicos y metodologías sobre aplicaciones y sistemas informáticos.
4. Plan de Capacitación Informática.
5. Informe de evaluación trimestral de Capacitación Informática.
6. Propuestas de políticas de gestión tecnológica.
7. Informes de implementación, administración y mantenimiento de aplicaciones y sistemas informáticos.
8. Términos de referencia y especificaciones técnicas.
9. Proyectos de adquisición de software propietario y software libre.
10. Informes de soporte informático y capacitación en aplicaciones y sistemas de información.

Seguridad Informática

a. Productos y Servicios

11. Procedimientos de accesos a datos y otros recursos.
12. Informe de seguridad y confidencialidad de identificaciones de usuario y contraseña.
13. Informe de monitoreo de violaciones de seguridad.
14. Informes periódicos de políticas de seguridad.
15. Informe de cumplimiento de procesos establecidos.
16. Informes de pruebas o revisiones de software.
17. Políticas de Seguridad de la información y comunicación.
18. Informes de aseguramiento y calidad de software.
19. Test de penetración al sistema operativo.
20. Test de penetración de redes y comunicaciones.
21. Afinamiento a los sistemas operativos.
22. Informe de implementación de antivirus.

3.2.1.6.2 Base de Datos

a. Productos y Servicios

1. Informe de cambio de la información física de datos.
2. Informe de implementación de herramientas de optimización.
3. Informe de consultas sobre la estructura de la base de datos.
4. Informe de implementación de controles de definición, acceso, actualización y concurrencia.

5. Informe de monitoreo de la base de datos.
6. Informes de definición de backups.
7. Informes de Auditoría de base de datos.
8. Informes de actualización del diccionario de datos.
9. Informes de actualización de la estructura de base de datos.

3.2.1.6.3 Aplicaciones Informáticas

a. Productos y Servicios

1. Plan Estratégico de la Unidad.
2. Informe de actividades y proyectos de desarrollo de sistemas de información destinadas al Plan Operativo Informático (POI).
3. Informes de ejecución de proyectos de desarrollo de sistemas informáticos aplicando estándares de desarrollo establecidos.
4. Plan Anual de Mantenimiento de Sistemas de información.
5. Informe de ejecución de actividades de mantenimiento de sistemas informáticos.
6. Especificaciones técnicas de los servicios de desarrollos informáticos y aplicativos.
7. Informe de evaluación y monitoreo de la ejecución de proyectos de desarrollo de sistemas informáticos realizados por terceros.
8. Informes de asistencia técnica sobre soluciones tecnológicas puestas a consideración por terceros.
9. Propuestas de tecnologías de información en los procesos del Ministerio de Transporte y Obras Públicas como resultado de investigaciones de carácter tecnológico.
10. Propuestas de políticas de seguridad informática en el ámbito de su competencia.
11. Informes de administración técnica de los sistemas informáticos y los manuales de usuarios de cada sistema informático del Ministerio.
12. Informes de los proyectos de desarrollo informático ejecutados y en ejecución.
13. Informes de asesoría a las unidades orgánicas en la identificación de soluciones que involucren el desarrollo o aplicación de sistemas informáticos.
14. Propuestas de gestión e implementación de mejoras e innovaciones en los procesos, procedimientos y normatividad relacionado con la unidad.

3.2.1.6.4 Soporte Técnico Informático

Mantenimiento

a. Productos y Servicios

1. Informes de administración de licencias de programas informáticos comerciales (software).
2. Inventario de equipos de cómputo (hardware).
3. Informes de administración del correo electrónico del Ministerio de Transporte y Obras Públicas.

4. Informes de administración del servicio de Internet.
5. Informes de administración del servicio de asistencia al usuario ("Help desk").
6. Informes de aplicación de políticas de seguridad informática.
7. Informes de mantenimiento preventivo y correctivo de los equipos de cómputo.
8. Informes de administración del Portal Web del Ministerio de Transporte y Obras Públicas.
9. Informes de administración de Activos Informáticos.
10. Reporte de actualizaciones del sistema operativo.
11. Estadísticas de malware (virus, gusanos, etc.).
12. Informes de actualización de antivirus.

Redes y Telecomunicaciones

a. Productos y Servicios

1. Informes de ejecución de proyectos de infraestructura tecnológica relacionados con redes y telecomunicaciones.
2. Propuestas de aplicación de tecnologías de comunicaciones en los procesos del Ministerio de Transporte y Obras Públicas, como resultados de investigaciones de carácter tecnológico.
3. Especificaciones técnicas de procesos de selección referidos a servicios o proyectos de telecomunicaciones.
4. Informes de supervisión de proyectos por terceros, relacionados con equipos de redes y comunicaciones.
5. Informes de administración de la red de datos (administración de usuarios, servidores y dispositivos de comunicaciones).
6. Informes de administración de la interconexión de locales, incluyendo la basada en tecnología inalámbrica.
7. Informes de administración de la red de telefonía.
8. Informes de aplicación de las políticas de seguridad informática en redes.
9. Informes de ejecución de actividades orientadas al cumplimiento de la normatividad gubernamental en materia de telecomunicaciones y protección de la propiedad intelectual.
10. Informes de monitoreo del tráfico en los canales de comunicación.

4. PROCESOS DESCONCENTRADOS

4.1 SUBSECRETARIA ZONAL DE TRANSPORTE Y OBRAS PÚBLICAS

4.1.1 PROCESO GOBERNANTE

4.1.1.1 GERENCIAMIENTO DE LA INFRAESTRUCTURA DEL TRANSPORTE ZONAL

a. **Misión.-** Planificar, aprobar, coordinar, controlar y evaluar el desarrollo e implementación de las políticas, planes, programas y proyectos de infraestructura del transporte; y la ejecución de los estudios contribuyendo al desarrollo económico y social de la zona.

ANEXO 2:

NORMAS DE CONTROL INTERNO

ACUERDO 039 – NORMA 410

Energía, es el recurso que se encuentra asociado al movimiento, conjuntamente con la materia, forma el cosmos.

La unidad de gestión ambiental, evaluará las manifestaciones de la energía, pues se la define únicamente en función de sus efectos, como la capacidad de efectuar un trabajo.

En el ambiente interesa fundamentalmente la manera de cómo la luz se relaciona con el conjunto de seres vivos y de cómo la energía es transformada dentro de esos seres.

410 TECNOLOGÍA DE LA INFORMACIÓN

410-01 Organización informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-02 Segregación de funciones

Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada unas de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

410–03 Plan informático estratégico de tecnología

La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario.

La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia. Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico.

El plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos serán analizados y aprobados por la máxima autoridad de la organización e incorporados al presupuesto anual de la organización; se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.

410-04 Políticas y procedimientos

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.

Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.

La unidad de tecnología de información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.

410-05 Modelo de información organizacional

La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.

El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentado de forma permanente, incluirá las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente.

Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad.

410-06 Administración de proyectos tecnológicos

La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

1. Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.

2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.

3. La formulación de los proyectos considerará el *Costo Total de Propiedad CTP*; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.

4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.

5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.

6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.

7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.

8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto.

9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.

10. El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

410-07 Desarrollo y adquisición de software aplicativo

La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.

3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.

4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la organización.

6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.

7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.

8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.

10. Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.

11. Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.

410-08 Adquisiciones de infraestructura tecnológica

La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.

3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.

4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante.

410-09 Mantenimiento y control de la infraestructura tecnológica

La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.

2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.

3. Control y registro de las versiones del software que ingresa a producción.

4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.

5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.

8. El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;

2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;

3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;

4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;

5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.

6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;

7. Consideración y disposición de sitios de procesamiento alternativos.

8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

410-11 Plan de contingencias

Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Los aspectos a considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.

2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.

3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.

4. Plan de recuperación de desastres que comprenderá:

   - Actividades previas al desastre (bitácora de operaciones)
   - Actividades durante el desastre (plan de emergencias, entrenamiento)
   - Actividades después del desastre.

5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.

6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.

7. El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

410-12 Administración de soporte de tecnología de información

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.

2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.

3. Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.

4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.

5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.

6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.

7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.

8. Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.

9. Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.

10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.

11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

410-13 Monitoreo y evaluación de los procesos y servicios

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

410-14 Sitio web, servicios de internet e intranet

Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

La unidad de tecnología de información considerará el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general.

410-15 Capacitación informática

Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

410-16 Comité informático

Para la creación de un comité informático institucional, se considerarán los siguientes aspectos:

- El tamaño y complejidad de la entidad y su interrelación con entidades adscritas.
- La definición clara de los objetivos que persigue la creación de un comité de informática, como un órgano de decisión, consultivo y de gestión que tiene como propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad.
- La conformación y funciones del comité, su reglamentación, la creación de grupos de trabajo, la definición de las atribuciones y responsabilidades de los miembros del comité, entre otros aspectos.

410-17 Firmas electrónicas

Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.

El uso de la firma electrónica en la administración pública se sujetará a las garantías, reconocimiento, efectos y validez señalados en estas disposiciones legales y su normativa secundaria de aplicación.

Las servidoras y servidores autorizados por las instituciones del sector público podrán utilizar la firma electrónica contenida en un mensaje de datos para el ejercicio y cumplimiento de las funciones inherentes al cargo público que ocupan.

Los aplicativos que incluyan firma electrónica dispondrán de mecanismos y reportes que faciliten una auditoría de los mensajes de datos firmados electrónicamente.

a) Verificación de autenticidad de la firma electrónica

Es responsabilidad de las servidoras y servidores de las entidades o dependencias del sector público verificar mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida sea emitido por una entidad de certificación de información acreditada y que el mismo se encuentre vigente.

b) Coordinación interinstitucional de formatos para uso de la firma electrónica

Con el propósito de que exista uniformidad y compatibilidad en el uso de la firma electrónica, las entidades del sector público sujetos a este ordenamiento coordinarán y definirán los formatos y tipos de archivo digitales que serán aplicables para facilitar su utilización.

Las instituciones públicas adoptarán y aplicar los estándares tecnológicos para firmas electrónicas que las entidades oficiales promulguen, conforme a sus competencias y ámbitos de acción.

c) Conservación de archivos electrónicos

Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservarán en su estado original en medios electrónicos seguros, bajo la responsabilidad del usuario y de la entidad que los generó. Para ello se establecerán políticas internas de manejo y archivo de información digital.

d) Actualización de datos de los certificados de firmas electrónicas

Las servidoras y servidores de las entidades, organismos y dependencias del sector público titulares de un certificado notificarán a la entidad de certificación de Información sobre cualquier cambio, modificación o variación de los datos que constan en la información proporcionada para la emisión del certificado.

Cuando un servidor público deje de prestar sus servicios temporal o definitivamente y cuente con un certificado de firma electrónica en virtud de sus funciones, solicitará a la entidad de certificación de información, la revocación del mismo, además, el superior jerárquico ordenará su cancelación inmediata.

El dispositivo portable seguro será considerado un bien de la entidad o dependencia pública y por tanto, a la cesación del servidor, será devuelto con la correspondiente acta de entrega recepción.

e) Seguridad de los certificados y dispositivos portables seguros

Los titulares de certificados de firma electrónica y dispositivos portables seguros serán responsables de su buen uso y protección. Las respectivas claves de acceso no serán divulgadas ni compartidas en ningún momento. El servidor solicitará la revocación de su certificado de firma electrónica cuando se presentare cualquier circunstancia que pueda comprometer su utilización.

f) Renovación del certificado de firma electrónica

El usuario solicitará la renovación del certificado de firma electrónica con la debida anticipación, para asegurar la vigencia y validez del certificado y de las actuaciones relacionadas con su uso.

g) Capacitación en el uso de las firmas electrónicas

La entidad de certificación capacitará, advertirá e informará a los solicitantes y usuarios de los servicios de certificación de información y servicios relacionados con la firma electrónica, respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de los servicios contratados. Esta capacitación facilitará la comprensión y utilización de las firmas electrónicas, en los términos que establecen las disposiciones legales vigentes.

ANEXO 3:

ANÁLISIS DE PROCESOS

PROCESO	DESCRIPCIÓN	Práctica (Gobierno/Gestión)Clave	Descripción	NCI ACUERDO 039
Evaluar, Orientar y Supervisar (EMD)				
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	EDM01.01 Evaluar el sistema de gobierno	Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de TI de la empresa.	410-01 (410-03) 410-04 (410-09) 410-12 (410-13) 410-16
		EDM01.02 Orientar el sistema de gobierno	Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras, procesos y prácticas para el gobierno de TI en línea con los principios,modelos para la toma de decisiones y niveles de autoridaddiseñados para el gobierno. Definir la información necesariapara una toma de decisiones informadas.	
		EDM01.03 Supervisar el sistema de gobierno	Supervisar la ejecución y la efectividad del gobierno deTI de la empresa. Analizar si el sistema de gobierno y losmecanismos implementados (incluyendo estructuras,principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI.	
EDM02 Asegurar la entrega de beneficios	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables	EDM02.01 Evaluar la entrega de valor	Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio en la dirección que necesita ser dada a la gestión para optimizar la creación de valor.	N/A
		EDM02.02 Orientar la optimización del valor	Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI a lo largo de todo su ciclo de vida económico.	
		EDM02.03 Supervisar la optimización del valor	Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando el valor y los beneficios previstos de los servicios e inversiones TI. Identificar los problemas significativos y considerar las acciones correctivas.	
EDM03 Asegurar la optimización del riesgo	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	EDM03.01 Evaluar la gestión de riesgos	Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de laempresa relacionado con el uso de TI es identificado y gestionado.	(410-03) 410-04 410-10 410-11
		EDM03.02 Orientar la gestión de riesgos	Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo.	
		EDM03.03 Supervisar la gestión de riesgos	Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.	
EDM04 Asegurar la optimización de recursos	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	EDM04.01 Evaluar la gestión de recursos	Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la empresa.	(410-02) 410-08 410-09
		EDM04.02 Orientar la gestión de recursos	Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos deTI a lo largo de su completo ciclo de vida económica.	
		EDM04.03 Supervisar la gestión de recursos	Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas.	
EDM05 Asegurar la transparencia hacia las partes interesadas	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas	Examinar y juzgar continuamente los requisitos actuales y futuros de comunicación con las partes interesadas y de la elaboración de informes, incluyendo tanto los requisitos obligatorios (p. ej. de regulación) de elaboración de informes como la comunicación a otros interesados. Establecer los principios de la comunicación.	N/A
		EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes	Garantizar el establecimiento de una comunicación y una elaboración de informes eficaces, incluyendo mecanismos para asegurar la calidad y la completitud de la información, vigilar la elaboración obligatoria de informes y crear una estrategia de comunicación con las partes interesadas.	
		EDM05.03 Supervisar la comunicación con las partes interesadas	Supervisar la eficacia de la comunicación con las partes interesadas. Evaluar los mecanismos para asegurar la precisión, la fiabilidad y la eficacia y determinar si se están cumpliendo los requisitos de los diferentes interesados.	
Alinear, Planear y Organizar (APO)				
		APO01.01 Definir la estructura organizativa	Establecer una estructura organizativa interna y extensa que refleje las necesidades del negocio y las prioridades de TI. Implementar las estructuras de gestión requeridas (p. ej., comités) para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.	
		APO01.02 Establecer roles y responsabilidades	Establecer, acordar y comunicar roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas, que reflejen claramente las necesidades generales del negocio y los objetivos de TI, así como la autoridad, las responsabilidades y la rendición de cuentas del personal relevante.	

APO01 Gestionar el marco de gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	APO01.03 Mantener los elementos catalizadores del sistema de gestión	Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa y garantizar que están integrados y alineados con la filosofía y el estilo operativo de gobierno y de gestión de la empresa. Estos elementos catalizadores incluyen una comunicación clara de expectativas/requisitos. El sistema de gestión debería fomentar la cooperación interdepartamental y el trabajo en equipo, promover el cumplimiento y la mejora continua y tratar las desviaciones en el proceso (incluidos los fallos).	410-01 410-02 410-03 410-06
		APO01.04 Comunicar los objetivos y la dirección de gestión	Comunicar la sensibilización y la comprensión de los objetivos y la dirección de TI a las partes interesadas yusuarios pertinentes a lo largo de toda la empresa.	
		APO01.05 Optimizar la ubicación de la función de TI	Posicionar la capacidad de TI en la estructura organizativa global para reflejar en el modelo de empresa la importancia de TI en la organización, especialmente su criticidad para la estrategia empresarial y el nivel de dependencia de TI. La línea de reporte del CIO debe ser proporcional a la importancia de las TI en la empresa.	
		APO01.06 Definir la propiedad de la información (datos) y del sistema	Definir y mantener las responsabilidades de la propiedadde la información (datos) y los sistemas de información.Asegurar que los propietarios toman decisiones sobre la clasificación de la información y los sistemas y su protección de acuerdo con esta clasificación.	
		APO01.07 Gestionar la mejora continua de los procesos	Evaluar, planificar y ejecutar la mejora continua de procesos y su madurez para asegurar que son capaces de entregarse conforme a los objetivos de la empresa, de gobierno, de gestión y de control. Considerar las directrices de la implementación de procesos de COBIT, estándares emergentes, requerimientos de cumplimiento, oportunidades de automatización y la realimentación de los usuarios de los procesos, el equipo del proceso y otras partes interesadas. Actualizar los procesos y considerar el impacto en los catalizadores del proceso.	
		APO01.08 Mantener el cumplimiento con las políticas y procedimientos	Poner en marcha procedimientos para mantener el cumplimiento y medición del funcionamiento de las políticas y otros catalizadores del marco de referencia; hacer cumplir las consecuencias del no cumplimiento o del desempeño inadecuado. Seguir las tendencias y el rendimiento y considerarlos en el diseño futuro y la mejora del marco de control.	
APO02 Gestionar la estrategia	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.	APO02.01 Comprender la dirección de la empresa	Considerar el entorno actual y los procesos de negocio de la empresa, así como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella (motivadores de la industria, reglamentos relevantes, bases para la competencia).	410-01 410-02 410-03 410-04
		APO02.02 Evaluar el entorno, cay rendimiento actuales	Evaluar el rendimiento del negocio interno actual y las capacidades de TI y los servicios externos de TI para desarrollar un entendimiento de la arquitectura empresarial en relación con TI. Identificarlos problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectosdiferenciadores y las opciones de proveedores de servicios y el impacto financiero, los costes y los beneficios potenciales de utilizar servicios externos.	
		APO02.03 Definir el objetivo de las capacidades de TI	Definir el objetivo del negocio, las capacidades de TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes o propuestas de innovación.	
		APO02.04 Realizar un análisis de diferencias	Identificar las diferencias entre el entorno actual y el deseado y considerar la alineación de activos (las capacidades que soportan los servicios) con los resultados de negocio para optimizar la inversión y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia.	
		APO02.05 Definir el plan estratégico y la hoja de ruta	Crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo losobjetivos de TI contribuirán a los objetivos estratégicosde la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar las tecnologías paradefinir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y lasmedidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel.	
		APO02.06 Comunicar la estrategia y la dirección de TI	Crear conciencia y comprensión del negocio y de losobjetivos y dirección de TI, como se encuentra reflejadaen la estrategia de TI, a través de comunicaciones a laspartes interesadas adecuadas y a los usuarios de todala empresa.	
	Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y	APO03.01 Desarrollar la visión de la arquitectura de empresa	La visión de la arquitectura proporciona una primera descripción de alto nivel de las arquitecturas de partida y objetivo, cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al promotor la herramienta clave para vender los beneficios de la capacidad propuesta a las partes interesadas de la empresa. La visión de la arquitectura de información describe como nuevas capacidades permitirán alcanzar las metas de la empresa y los objetivos estratégicos y considera la preocupaciones de las partes interesadas en su implementación.	
		APO03.02 Definir la arquitectura de referencia	La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología.	

APO03 Gestionar la arquitectura empresarial	eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.	APO03.03 Seleccionar las oportunidades y las soluciones	Racionalizar las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica como la del negocio y agrupándolos a ambos en paquetes de trabajo del proyecto. Integrar el proyecto con todos los programas de inversión relacionados con TI para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que estas iniciativas sean parte del cambio general en la empresa. Hacer de ello un esfuerzo en colaboración con las partes interesadas clave de la empresa y en TI para evaluar el grado de preparación de la empresa para su transformación e identificar las oportunidades, soluciones y todas las restricciones de la implementación.	N/A
		APO03.04 Definir la implantación de la arquitectura	Crear un plan de implementación y de migración viable acorde con la cartera de proyectos y programas. Asegurarse que el plan está coordinado de cerca para asegurar que se proporciona el valor y que se disponen de los recursos necesarios para finalizar los trabajos.	
		APO03.05 Proveer los servicios de arquitectura empresarial	La provisión de los servicios de arquitectura empresarial incluye las guías y supervisión de los proyectos a implementar, la formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y comunicación de los valores aportados por la arquitectura y la supervisión del cumplimiento.	
APO04 Gestionar la Innovación	Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.	APO04.01 Crear un entorno favorable para la innovación	Crear un entorno que sea propicio para la innovación, considerando la cultura, la gratificación, la colaboración, los foros tecnológicos y los mecanismos para promover y captar ideas de los empleados.	N/A
		APO04.02 Mantener un entendimiento del entorno de la empresa	Trabajar junto a las partes interesadas para entender sus retos. Mantener un entendimiento adecuado de la estrategia corporativa y del entorno competitivo, así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.	
		APO04.03 Supervisar y explorar el entorno tecnológico	Realizar una supervisión sistemática y un escaneo del entorno externo a la empresa para identificar tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, realizando la estrategia corporativa, optimizando costes, evitando la obsolescencia y catalizando de una mejor manera los procesos corporativos y de TI). Supervisar el mercado, la competencia, sectores industriales y tendencias legales y regulatorias que permitan analizar tecnologías emergentes o ideas innovadoras en el contexto empresarial.	
		APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras	Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación TI. Trabajar con las partes interesadas para validar las suposiciones sobre el potencial de las nuevas tecnologías y la innovación.	
		APO04.05 Recomendar iniciativas apropiadas adicionales	Evaluar y supervisar los resultados de las pruebas de concepto y, si son favorables, generar recomendaciones para más iniciativas y obtener el soporte de las partes interesadas.	
		APO04.06 Supervisar la implementación y el uso de la innovación	Supervisar la implementación y el uso de las tecnologías emergentes durante la integración, adopción y durante todo el ciclo de vida económico para garantizar que se producen los beneficios prometidos y para identificar las lecciones aprendidas.	
APO05 Gestionar el portafolio	Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.	APO05.01 Establecer la mezcla del objetivo de inversión	Revisar y garantizar la claridad de las estrategias y servicios actuales corporativos y de TI. Definir una adecuada mezcla de inversión, basada en los costes, la alineación con la estrategia y medidas financieras, tales como coste, retorno de inversión esperado a lo largo de todo el ciclo de vida económico, grado de riesgo y tipo de beneficio para los programas del portafolio. Ajustar las estrategias corporativas y de TI cuando sea necesario.	410-07 410-08 410-13
		APO05.02 Determinar la disponibilidad y las fuentes de fondos	Determinar las fuentes potenciales de fondos, diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas del retorno de inversión.	
		APO05.03 Evaluar y seleccionar los programas a financiar	Basado en los requisitos de la mezcla general del portafolio de inversión, evaluar y priorizar casos de negocio de programas y decidir sobre las propuestas de inversión. Dedicar fondos e iniciar los programas.	
		APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones	Regularmente, supervisar y optimizar el rendimiento del portafolio de inversiones y de los programas individuales a lo largo de todo el ciclo de vida de inversión.	
		APO05.05 Mantener los portafolios	Mantener los portafolios de programas y proyectos deinversión, servicios de TI y activos de TI.	
		APO05.06 Gestionar la consecución de beneficios	Supervisar los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas, basadas en el caso de negocio acordado actual.	
APO06 Gestionar el presupuesto y los costos	Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y	APO06.01 Gestionar las finanzas y la contabilidad	Establecer y mantener un método de contabilización para todos los costes, inversiones y depreciaciones relacionadas con las TI, como parte integral de los sistemas financieros empresariales y el plan de cuentas para administrar las inversiones y los costes de TI. Capturar y asignar los costes reales, analizar las desviaciones entre las previsiones y los costes reales, e informar usando los sistemas empresariales de medición financiera.	
		APO06.02 Priorizar la asignación de recursos	Implementar un proceso de toma de decisiones para priorizar la asignación de recursos y definir las reglas para las inversiones discrecionales por parte de unidades de negocio individuales. Incluir el uso potencial de proveedores de servicio externos y considerar las opciones de compra, desarrollo y alquiler.	
		APO06.03 Crear y mantener presupuestos	Preparar un presupuesto que refleje las prioridades de inversión que apoyen los objetivos estratégicos basado en la cartera de programas habilitados por TI y servicios de TI.	N/A

	empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.	APO06.04 Modelar y asignar costes	Establecer y utilizar un modelo de costes de TI basado en la definición del servicio, asegurando que la asignación de costes de los servicios es identificable, medible y predecible, para fomentar el uso responsable de los recursos, incluyendo aquellos proporcionados por proveedores de servicio. Revisar regularmente y comparar la idoneidad del modelo de costes/prorrateo de costes para mantener su pertinencia y adecuación al negocio en evolución y las actividades de TI que le dan soporte.	
		APO06.05 Gestionar costes	Implementar un proceso de gestión de costes comparando los costes reales con los presupuestos. Los costes deben ser supervisados y comunicados y, en el caso de desviaciones, identificados oportunamente, así como evaluado su impacto en los procesos y servicios empresariales.	
APO07 Gestionar los recursos humanos	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	APO07.01 Mantener la dotación de personal suficiente y adecuada	Evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos para asegurar que la empresa tiene suficientes recursos humanos para apoyar las metas y objetivos empresariales. El personal incluye recursos tanto internos como externos.	410-02 410-04 410-15
		APO07.02 Identificar personal clave de TI	Identificar el personal clave de TI a la vez que se reduce al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento (documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (backup) del personal.	
		APO07.03 Mantener las habilidades y competencias del personal	Definir y gestionar las habilidades y competencias necesarias del personal. Verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso. Proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.	
		APO07.04 Evaluar el desempeño laboral de los empleados	Lleve a cabo oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias. Los empleados deberían recibir preparación sobre el desempeño y conducta siempre que sea apropiado.	
		APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio	Comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa. Identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI.	
		APO07.06 Gestionar el personal contratado	Asegúrese de que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conocen y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados.	
APO08 Gestionar las relaciones	Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.	APO08.01 Entender las expectativas del negocio	Entender el enfoque y expectativas actuales del negocio para TI. Asegurar que los requisitos son entendidos, gestionados y comunicados y su estado acordado y aprobado.	N/A
		APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio	Identificar oportunidades potenciales para que la TI sea catalizadora de la mejora del rendimiento empresarial.	
		APO08.03 Gestionar las relaciones con el negocio	Gestionar la relación con los clientes (representantes del negocio). Asegurar que los roles y responsabilidades de la relación están definidos, asignados y se facilita la comunicación.	
		APO08.04 Coordinar y comunicar	Trabajar con las partes interesadas y coordinar de extremo a extremo la entrega de los servicios TI y las soluciones proporcionadas al negocio.	
		APO08.05 Proveer datos de entrada para la mejora continua de los servicios	Mejorar y evolucionar continuamente los servicios basados en TI y la entrega del servicio a la empresa para alinearlos con unos cambiantes requisitos de empresa y tecnológicos.	
APO09 Gestionar los acuerdos de servicio	Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, i+ncluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.	APO09.01 Identificar servicios TI	Analizar los requisitos del negocio y el modo en que los servicios TI y los niveles de servicio soportan los procesos de negocio. Discutir y acordar servicios potenciales y niveles de servicio con el negocio y compararlos con la cartera actual para identificar servicios nuevos o modificados, u opciones de nivel de servicio.	N/A
		APO09.02 Catalogar servicios basados en TI	Definir y mantener uno o más catálogos de servicios para grupos de clientes objetivo relevantes. Publicar y mantener los servicios TI activos en los catálogos.	
		APO09.03 Definir y preparar acuerdos de servicio	Definir y preparar los acuerdos de servicio basándose en las opciones de los catálogos de servicio. Incluir acuerdos de nivel de operaciones interno.	
		APO09.04 Supervisar e informar de los niveles de servicio	Supervisar los niveles de servicio, informar de las mejoras e identificar tendencias. Proporcionar información de gestión adecuada para ayudar a la gestión del rendimiento.	
		APO09.05 Revisar acuerdos de servicio y contratos	Llevar a cabo revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.	
APO10 Gestionar los	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las	APO10.01 Identificar y evaluar las relaciones y contratos con proveedores	Identificar proveedores y contratos asociados y categorizarlos por tipo, relevancia y criticidad. Establecer un criterio de evaluación de contratos y proveedores y evaluar la cartera general de proveedores y contratos actuales y alternativos.	
		APO10.02 Seleccionar proveedores	Seleccionar proveedores de acuerdo a prácticas justas y formales que aseguren la selección del que mejor se adapte a los requisitos. Los requisitos deberían estar optimizados con las aportaciones de nuevos proveedores potenciales.	

APO10 Gestionar los proveedores	Incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.	APO10.03 Gestionar contratos y relaciones con proveedores	Formalizar y gestionar las relaciones con cada proveedor. Gestionar, mantener y supervisar los contratos y la entrega de servicios. Asegurar que los nuevos contratos o los cambios son conformes a las normas de la empresa, las leyes y las regulaciones. Gestionar los conflictos contractuales.	N/A
		APO10.04 Gestionar el riesgo en el suministro	Identificar y gestionar los riesgos relacionados con la capacidad de los proveedores de proporcionar de manera continua una entrega del servicio segura, eficaz y eficiente.	
		APO10.05 Supervisar el cumplimiento y el rendimiento del proveedor	Revisar periódicamente el rendimiento general de los proveedores, el cumplimiento con los requisitos contractuales y el valor de lo pagado y tratar las incidencias identificadas.	
APO11 Gestionar la calidad	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.	APO11.01 Establecer un sistema de gestión de la calidad (SGC)	Establecer y mantener un SGC que proporcione una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo.	N/A
		APO11.02 Definir y gestionar los estándares, procesos y prácticas de calidad	Identificar y mantener los requisitos, normas, procedimientos y prácticas de los procesos clave para orientar a la organización en el cumplimiento del SGC. Este debería estar en consonancia con los requisitos del marco de control TI. Considerar la posibilidad de certificar los procesos, las unidades de la organización, los productos o los servicios clave.	
		APO11.03 Enfocar la gestión de la calidad en los clientes.	Enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de calidad.	
		APO11.04 Supervisar y hacer controles y revisiones de calidad.	Supervisar la calidad de los procesos y servicios de forma permanente como se defina en el SGC. Definir, planificar y aplicar medidas para supervisar la satisfacción del cliente con la calidad, así como el valor que proporciona el SGC. La información recogida debería ser utilizada por los propietarios de los procesos para mejorar la calidad.	
		APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	Incorporar las prácticas pertinentes de gestión de la calidad en la definición, supervisión, notificación y gestión continua de los desarrollo de soluciones y los servicios ofrecidos.	
		APO11.06 Mantener una mejora continua	Mantener y comunicar regularmente un plan de la calidad global que promueva la mejora continua. Esto debería incluir la necesidad y los beneficios de una mejora continua. Recoger y analizar datos sobre el SGC y mejorar su eficacia. Corregir las no conformidades para prevenir la recurrencia. Promover una cultura de mejora continua de la calidad.	
APO12 Gestionar el riesgo	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	APO12.01 Recopilar datos	Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.	410-04 410-11 410-12
		APO12.02 Analizar el riesgo	Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.	
		APO12.03 Mantener un perfil de riesgo	Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.	
		APO12.04 Expresar el riesgo	Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada.	
		APO12.05 Definir un portafolio de acciones para la gestión de riesgos	Gestionar las oportunidades para reducir el riesgo a unnivel aceptable como un portafolio.	
		APO12.06 Responder al riesgo	Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.	
APO13 Gestionar la seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	APO13.01 Establecer y mantener un SGSI	Establecer y mantener un SGSI que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que esté alineados con los requerimientos de negocio y la gestión de seguridad en la empresa.	410-10
		APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información	Mantener un plan de seguridad de información que describa cómo se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de empresa. Asegurar que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocio aprobados, se implementan como parte integral del desarrollo de soluciones y servicios y se operan, después, como parte integral de las operaciones del negocio.	
		APO13.03 Supervisar y revisar el SGSI	Mantener y comunicar regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad. Corregir las no conformidades para prevenir recurrencias. Promover una cultura de seguridad y de mejora continua.	
Construir, Adquirir e Implementar (BAI)				
		BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos	Mantener un enfoque estándar para la gestión de programas y proyectos que posibilite revisiones y tomas de decisión de gobierno y de gestión y actividades de gestión de la entrega, enfocadas en la consecución de valor y de objetivos (requisitos, riesgos, costes, cronograma y calidad) para el negocio de una forma consistente.	

BAI01 Gestionar programas y proyectos	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.	BAI01.02 Iniciar un programa	Iniciar un programa para confirmar los beneficios esperados y para obtener la autorización para proceder. Esto incluye los acuerdos sobre el patrocinio del programa, confirmar el mandato del programa a través de la aprobación del caso de negocio conceptual, designar a los consejeros o los miembros del comité del programa, generar el expediente del programa, revisar y actualizar el caso de negocio, desarrollar un plan de realización de beneficios y obtener la aprobación de los patrocinadores para empezar.	410-06
		BAI01.03 Gestionar el compromiso de las partes interesadas	Gestionar el compromiso de las partes interesadas para asegurar un intercambio activo de información precisa, consistente y oportuna, que llegue a todos las partes interesadas relevantes. Esto incluye la planificación, identificación y el compromiso de las partes interesadas y la gestión de sus expectativas.	
		BAI01.04 Desarrollar y mantener el plan de programa	Formular un programa para definir las bases iniciales y posicionarlo para una ejecución exitosa mediante la formalización del alcance del trabajo a ser efectuado e identificando los entregables que satisfarán sus objetivos y la entrega de valor. Mantener y actualizar el plan del programa y el caso de negocio a lo largo del ciclo de vida económico completo del programa, asegurando el alineamiento con los objetivos estratégicos y reflejando el estado actual y los conocimientos obtenidos hasta el momento.	
		BAI01.05 Lanzar y ejecutar el programa	Lanzar y ejecutar el programa para adquirir y dirigir los recursos necesarios para lograr las metas y beneficios definidos en el plan del programa. De acuerdo con los criterios de revisión de lanzamiento o cambio de fase (stage-gate), preparar los cambios de fase, las revisiones de las iteraciones o versiones para informar del progreso del programa y ser capaz de establecer los fundamentos para la financiación de la siguiente etapa después de la revisión del lanzamiento o de cambio de fase (stage-gate).	
		BAI01.06 Supervisar, controlar e informar de los resultados del programa	Supervisar y controlar el rendimiento del programa (entrega de soluciones) y de la organización (valor/resultado) versus el plan durante el ciclo de vida económico completo de la inversión. Informar del rendimiento al comité estratégico del programa y a los patrocinadores.	
		BAI01.07 Lanzar e iniciar proyectos dentro de un programa	Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar entre las partes interesadas un entendimiento común o el alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa general de inversiones de TI. La definición debería estar formalmente aprobada por el patrocinador del programa y del proyecto.	
		BAI01.08 Planificar proyectos	Establecer y mantener un plan de proyecto formal, aprobado e integrado (que cubra los recursos del negocio y de TI), para guiar la ejecución del proyecto y controlarlo durante toda su vida. El alcance de los proyectos debería estar claramente definido y vinculado claramente a la construcción o aumento de la capacidad del negocio.	
		BAI01.09 Gestionar la calidad de los programas y proyectos	Preparar y ejecutar un plan y procesos y prácticas de gestión de la calidad, alineadas al SGC que describe el enfoque de calidad del programa y el proyecto y cómo será implementado. El plan debería ser formalmente revisado y acordado por todas las partes afectadas y, después, incorporado en los planes integrados del programa y los proyectos.	
		BAI01.10 Gestionar el riesgo de los programas y proyectos	Eliminar o minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Los riesgos enfrentados por la administración del programa y los proyectos deberían ser establecidos y registrados en un único punto.	
		BAI01.11 Supervisar y controlar proyectos	Medir el desempeño del proyecto versus los criterios clave de rendimiento del proyecto, tales como la planificación, la calidad, el coste y los riesgos. Evaluar el impacto de las desviaciones en el proyecto y el programa general e informar los resultados a las partes interesadas clave.	
		BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto	Gestionar los paquetes de trabajo mediante requerimientos formales de autorización y aceptación de los paquetes de trabajo, y asignando y coordinado los recursos de negocio y de TI adecuados.	
		BAI01.13 Cerrar un proyecto o iteración	Solicitar a las partes interesadas del proyecto, al final de cada proyecto, versión o iteración, que evalúen si el proyecto, la versión o la iteración entregaron los resultados y valorplaneados. Identificar y comunicar cualquier actividad pendiente necesaria para lograr los resultados del proyecto y los beneficios del programa planeados, identificar y documentar las lecciones aprendidas para futuros proyectos, versiones, iteraciones y programas.	
		BAI01.14 Cerrar un programa	Eliminar el programa del portafolio de inversiones activas cuando haya acuerdo de que el valor deseado ha sido logrado o cuando esté claro que no será logrado con los criterios de valor establecidos para el programa.	
BAI02 Gestionar la	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos,	BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio	Basándose en el caso de negocio, identificar, priorizar, especificar y acordar los requerimientos de información de negocio, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados de la solución de negocio de TI propuesta.	410-06
		BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas	Realizar un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida. Si se considera, implementar la opción seleccionada como un piloto para determinar posibles mejoras.	

definición de requisitos	infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.	BAI02.03 Gestionar los riesgos de los requerimientos	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la empresa y solución propuesta.	410-07
		BAI02.04 Obtener la aprobación de los requerimientos y soluciones	Coordinar la realimentación de las partes interesadas afectadas y, en las fases clave predeterminadas, obtener la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas.	
BAI03 Gestionar la identificación y construcción de soluciones	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.	BAI03.01 Diseñar soluciones de alto nivel	Desarrollar y documentar diseños de alto nivel usando técnicas de desarrollo ágil o por fases apropiadas y acordadas. Asegurar el alineamiento con la estrategia TI y la arquitectura empresarial. Revalorar y actualizar los diseños cuando sucedan cuestiones significativas durante las fases de diseño detallado o de construcción o según la solución evolucione. Asegurar que las partes interesadas participen activamente en el diseño y en la aprobación de cada versión.	N/A
		BAI03.02 Diseñar los componentes detallados de la solución	Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previamente considerando todos los componentes (procesos de negocio y automatización relacionada y controles manuales, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes). Asegurar que el diseño detallado incluye ANSs y OLAs internos y externos	
		BAI03.03 Desarrollar los componentes dela solución	Desarrollar, documentar y elaborar diseños detallados progresivamente usando técnicas de desarrollo ágiles o por fases acordadas previamente considerando todos los componentes (procesos de negocio y automatización relacionada y controles manuales, aplicaciones soporte de TI, servicios de infraestructura y productos tecnológicos y proveedores/fabricantes). Asegurar que el diseño detallado incluye ANSs y OLAs internos y externos	
		BAI03.04 Obtener los componentes de la solución	Obtener los componentes de la solución sobre la base del plan de adquisiciones y conforme a los requerimientos y diseños detallados, principios de arquitectura y estándares y en los procedimientos generales contractuales y de adquisiciones de la empresa, requerimientos de calidad (QA) y aprobación de estándares. Asegurar que todos los requerimientos legales y contractuales son identificados y cumplidos por el proveedor.	
		BAI03.05 Construir soluciones	Instalar y configurar las soluciones e integrarlas con lasactividades de los procesos de negocio. Implementar controles, medidas de seguridad y 'auditabilidad' durante la configuración y durante la integración del hardware e infraestructura del software para proteger los recursos y asegurar la disponibilidad e integridad de los datos. Actualizar el catálogo de servicios para reflejar la nueva situación.	
		BAI03.06 Realizar controles de calidad	Desarrollar y ejecutar un plan de calidad (QA) alineado con el SGC para obtener la calidad especificada en la definición de los requerimientos y de acuerdo a las políticas y procedimientos de calidad de la empresa.	
		BAI03.07 Preparar pruebas de la solución	Establecer un plan de pruebas y entornos necesarios para probar los componentes individualmente y de la solución integrada incluyendo los procesos de negocio y servicios, aplicaciones e infraestructura que los soportan.	
		BAI03.08 Ejecutar pruebas de la solución	Ejecutar pruebas continuamente durante el desarrollo, incluyendo pruebas de control, en concordancia con e plan de pruebas y con las prácticas de desarrollo en el entono apropiado. Hacer partícipes a los dueños de los procesos de negocio y usuarios finales en el equipo de pruebas. Identificar, registrar y priorizar los errores e incidentes identificados durante las pruebas.	
		BAI03.09 Gestionar cambios a los requerimientos	Hacer seguimiento del estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) a través de todo el ciclo de vida del proyecto y gestionar la aprobación de los cambios a los requerimientos.	
		BAI03.10 Mantener soluciones	Desarrollar y ejecutar un plan para el mantenimiento de la solución y componentes de la infraestructura. Incluir revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales.	
		BAI03.11 Definir los servicios TI y mantener el catálogo de servicios	Definir y acordar nuevos servicios TI o cambios y opciones de nivel de servicio. Documentar nuevas definiciones o cambios en los servicios y opciones de nivel de servicio que serán actualizadas en el catálogo de servicios.	
BAI04 Gestionar la disponibilidad y capacidad	Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos	BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia	Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costes para dar soporte a las necesidades del negocio y para entregar el servicio deacuerdo a los ANSs. Crear líneas de referencia para la disponibilidad, el rendimiento y la capacidad para comparaciones futuras.	410-08 410-09
		BAI04.02 Evaluar el impacto en el negocio	Identificar los servicios importantes para la empresa, mapear los servicios y recursos con los procesos de negocio e identificar las dependencias del negocio. Asegurar que el impacto de la indisponibilidad de recursos está acordado y aceptado por el cliente. Asegurar que, para las funciones vitales del negocio, los requisitos de disponibilidad definidos en el ANS pueden ser satisfechos.	
		BAI04.03 Planificar requisitos de servicio nuevos o modificados	Planificar y priorizar las implicaciones en la disponibilidad, el rendimiento y la capacidad de cambios en las necesidades del negocio y en los requerimientos de servicio	

	Implementar acciones para alcanzar los requerimientos identificados. Declaración del Propósito del Proceso	BAI04.04 Supervisar y revisar la disponibilidad y la capacidad	Supervisar, medir, analizar, informar y revisar la disponibilidad, el rendimiento y la capacidad. Identificar desviaciones respecto a las líneas de referencia establecidas. Revisar informes de análisis de tendencias identificando cualquier cuestión y variación significativa, iniciando acciones donde sea necesario y asegurando que se realiza el seguimiento de todas las cuestiones pendientes.	
		BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad	Abordar las desviaciones investigando y resolviendo las cuestiones identificadas relativas a disponibilidad, rendimiento y capacidad.	
BAI05 Gestionar la introducción del cambio organizativo	Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI.	BAI05.01 Establecer el deseo de cambiar	Comprender el alcance e impacto del cambio divisado y la disposición/voluntad de cambiar de las partes interesadas. Identificar las acciones para motivar a las partes interesadas para aceptar y querer que el cambio sea exitoso.	
		BAI05.02 Formar un equipo de implementación efectivo	Establecer un equipo de implementación efectivo, con miembros adecuados, creando confianza y estableciendo metas comunes y medidas efectivas.	
		BAI05.03 Comunicar la visión deseada	Comunicar la visión deseada para el cambio en el lenguaje de aquellos que se verán afectados. La comunicación debería ser realizada por la alta dirección e incluir la razón de ser y los beneficios del cambio, el impacto de no hacerlo y la visión, la hoja de ruta y la participación requerida de las diversas partes interesadas.	
		BAI05.04 Facultar a los que juegan algún papel e identificar ganancias en el corto plazo	Facultar a aquellos con roles en la implementación asegurando que se han asignado responsabilidades, se ha dado formación y se han alineado las estructuras organizativas y procesos de RRHH. Identificar y comunicar ganancias en el corto plazo que pueda ser realizadas y resulten importantes desde una perspectivade posibilitar el cambio.	
		BAI05.05 Facilitar la operación y el uso	Planificar e implementar todos los aspectos técnicos,operativos y de modo de uso de forma que todos aquellos involucrados en el entorno futuro puedan ejercer sus responsabilidades.	
		BAI05.06 Integrar nuevos enfoques	Integrar nuevos enfoques mediante el seguimiento de los cambios implementados, asegurando la efectividad del plan de operación y uso y manteniendo un plan de concienciación mediante comunicaciones regulares. Aplicar las medidas correctoras que se estime apropiado y que podrían incluir el forzar el cumplimiento.	
		BAI05.07 Mantener los cambios	Mantener los cambios mediante la formación eficaz del personal nuevo, campañas de comunicación periódicas, compromiso de la alta dirección, supervisión de la adopción de los cambios y divulgación a toda la empresa de las lecciones aprendidas.	
BAI06 Gestionar los cambios	Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.	BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio	Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados.	N/A
		BAI06.02 Gestionar cambios de emergencia	Gestionar cuidadosamente los cambios de emergencia para minimizar futuras incidencias y asegurar que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio.	
		BAI06.03 Hacer seguimiento e informar de cambios de estado	Mantener un sistema de seguimiento e informe que documente los cambios rechazados, comunique el estado de cambios aprobados y en proceso y de cambios completados. Asegurar que los cambios aprobados son implementados como esté previsto.	
		BAI06.04 Cerrar y documentar los cambios	Siempre que el cambio haya sido implementado, actualizar, de manera consecuente, la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.	
BAI07 Gestionar la aceptación del cambios y la transiciones	Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación	BAI07.01 Establecer un plan de implementación	Establecer un plan de implementación que cubra la conversión de datos y sistemas, criterios de aceptación de las pruebas, comunicación, formación, preparación del lanzamiento, paso a producción, soporte inicial en producción, plan de marcha atrás o de contingencia y una revisión post-implantación. Obtener la aprobación de las partes relevantes.	N/A
		BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos	Preparar la migración de procesos de negocio, datos de los servicios de TI e infraestructuras como parte de los mecanismos de desarrollo de la empresa, incluyendo registros de auditoría y un plan de recuperación para el caso de que la migración fallara.	
		BAI07.03 Planificar pruebas de aceptación	Establecer un plan de pruebas basado en estándares corporativos que defina roles, responsabilidades, y criterios de entrada y salida. Asegurar que el plan es aprobado por las partes relevantes.	
		BAI07.04 Establecer un entorno de pruebas	Definir y establecer un entorno seguro de pruebas que sea representativo del proceso de negocio y entorno de operaciones de TI planeados, en cuanto a rendimiento y capacidad, seguridad, controles internos, prácticas de operación, calidad de los datos y requisitos de privacidad y carga de trabajo.	
		BAI07.05 Ejecutar pruebas de aceptación	Probar los cambios independientemente, de acuerdo con el plan de pruebas definido, antes de migrar al entorno de producción.	
		BAI07.06 Pasar a producción y gestionarlos lanzamientos	Pasar la solución aceptada al negocio y las operaciones. Donde sea apropiado, ejecutar la solución como un proyecto piloto o en paralelo con la solución antigua durante un período de tiempo definido y comparar su comportamiento y resultados. Si se dieran problemas significativos, reinstaurar el entorno original de acuerdo al plan de marcha atrás o alternativo. Gestionar los lanzamientos de los componentes de la solución.	

		BAI07.07 Proporcionar soporte en producción desde el primer momento	Proporcionar soporte desde el primer momento a los usuarios y a las operaciones de TI durante un periodo de tiempo acordado para tratar cualquier incidencia y ayudar a estabilizar la nueva solución.	
BAI08 Gestionar el conocimiento	Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.	BAI08.01 Cultivar y facilitar una cultura de intercambio de conocimientos	Concebir e implantar un esquema para cultivar y facilitar una cultura de intercambio de conocimientos.	410-05
		BAI08.02 Identificar y clasificar las fuentes de información	Identificar, validar y clasificar las diversas fuentes de información interna y externa necesarias para posibilitar el uso y la operación efectivas de los procesos de negocio y los servicios de TI.	
		BAI08.03 Organizar y contextualizar la información, transformándola en conocimiento	Organizar la información basándose en criterios de clasificación. Identificar y crear relaciones significativasentre elementos de información y facilitar el uso de la información. Identificar propietarios y definir e implementar niveles de acceso a los recursos de información.	
		BAI08.04 Utilizar y compartir el conocimiento	Difundir las fuentes de conocimiento disponibles entre las partes interesadas relevantes y comunicar cómo estos recursos pueden ser utilizados para tratar diferentes necesidades (ej. resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).	
		BAI08.05 Evaluar y retirar la información	Medir el uso y evaluar la actualización y relevancia de la información. Retirar la información obsoleta.	
BAI09 Gestionar los activos	Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para le negocio y que el software instalado cumple con los acuerdos de licencia.	BAI09.01 Identificar y registrar activos actuales	Mantener un registro actualizado y exacto de todos los activos de TI necesarios para la prestación de servicios y garantizar su alineación con la gestión de la configuración y la administración financiera.	410-08 410-09 410-12
		BAI09.02 Gestionar activos críticos	Identificar los activos que son críticos en la provisión de capacidad de servicio y dar los pasos para maximizar su fiabilidad y disponibilidad para apoyar las necesidades del negocio.	
		BAI09.03 Gestionar el ciclo de vida de los activos	Gestionar los activos desde su adquisición hasta sueliminación para asegurar que se utilizan tan eficaz yeficientemente como sea posible y son contabilizados yprotegidos físicamente.	
		BAI09.04 Optimizar el coste de los activos	Revisar periódicamente la base global de activos para identificar maneras de optimizar los costes y mantener el alineamiento con las necesidades del negocio.	
		BAI09.05 Administrar licencias	Administrar las licencias de software de forma que semantenga el número óptimo de licencias para soportarlos requerimientos de negocio y el número de licenciasen propiedad sea suficiente para cubrir el softwareinstalado y en uso.	
BAI10 Gestionar la configuración	Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.	BAI10.01 Establecer y mantener un modelo de configuración	Establecer y mantener un modelo lógico de la infraestructura, activos y servicios y la forma de registrar los elementos de configuración (CIs del inglés, configuration items) y las relaciones entre ellos. Incluyendo los CIs considerados necesarios para gestionar eficazmente los servicios y proporcionar una sola descripción fiable de los activos en un servicio.	N/A
		BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia	Establecer y mantener un repositorio de gestión de la configuración y crear unas bases de referencia de configuración controladas.	
		BAI10.03 Mantener y controlar los elementos de configuración	Mantener un repositorio actualizado de elementos deconfiguración rellenado con los cambios.	
		BAI10.04 Generar informes de estado y configuración	Definir y elaborar informes de configuración sobre cambios en el estado de los elementos de configuración.	
		BAI10.05 Verificar y revisar la integridad del repositorio de configuración	Revisar periódicamente el repositorio de configuracióny verificar la integridad y exactitud con respecto alobjetivo deseado.	
Entregar, Servir y Dar Soporte(DSS)				
DSS01 Gestionar operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	DSS01.01 Ejecutar procedimientos operativos	Mantener y ejecutar procedimientos y tareas operativas de forma confiable y consistente.	410-08 410-10 410-11 410-13
		DSS01.02 Gestionar servicios externalizados de TI	Gestionar la operación de servicios externalizados de TI paramantener la protección de la información empresarial y la confiabilidad de la entrega del servicio.	
		DSS01.03 Supervisar la infraestructura de TI	Supervisar las infraestructura TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones.	
		DSS01.04 Gestionar el entorno	Mantener las medidas para la protección contra factores ambientales. Instalar equipamiento y dispositivos especializados para supervisar y controlar el entorno.	
		DSS01.05 Gestionar las instalaciones	Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.	
DSS02 Gestionar peticiones e incidentes de servicio.	Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio	Definir esquemas y modelos de clasificación de incidentes y peticiones de servicio.	N/A
		DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes	Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.	
		DSS02.03 Verificar, aprobar y resolver peticiones de servicio	Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.	
		DSS02.04 Investigar, diagnosticar y localizar incidentes	Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.	
		DSS02.05 Resolver y recuperarse de incidentes	Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.	

		DSS02.06 Cerrar peticiones de servicio e incidentes	Verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.	
		DSS02.07 Seguir el estado y emitir informes	Hacer seguimiento, analizar e informar de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua.	
DSS03 Gestionar problemas	Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.	DSS03.01 Identificar y clasificar problemas	Definir e implementar criterios y procedimientos para informar de los problemasidentificados, incluyendo clasificación, categorización y priorización de problemas.	N/A
		DSS03.02 Investigar y diagnosticar problemas	Investigar y diagnosticar problemas utilizando expertos en las materias relevantes para valorar y analizar las causas raíz.	
		DSS03.03 Levantar errores conocidos	Tan pronto como las causas raíz de los problemas se hayan identificado, crear registros de errores conocidos y una solución temporal apropiada, e identificar soluciones potenciales.	
		DSS03.04 Resolver y cerrar problemas	Identificar e iniciar soluciones sostenibles refiriéndose a la causa raíz, levantando peticionesde cambio a través del proceso de gestión de cambios establecido si se requiere para resolver errores. Asegurarse de que el personal afectado está al tanto de las acciones tomadas y de los planes desarrollados para prevenir que vuelvan aocurrir futuros incidentes.	
		DSS03.05 Realizar una gestión de problemas proactiva	Recoger y analizar datos operacionales (especialmente registros de incidentes y cambios) para identificar tendencias emergentes que puedan indicar problemas. Registrar problemas para permitir la valoración.	
DSS04 Gestionar la continuidad	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	DSS04.01 Definir la política de continuidad del negocio, objetivos y alcance	Definir la política y alcance de continuidad de negocioalineada con los objetivos de negocio y de las partes interesadas.	410-11
		DSS04.02 Mantener una estrategia de continuidad	Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.	
		DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio	Desarrollar un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas.	
		DSS04.04 Ejercitar, probar y revisar el plan de continuidad	Probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.	
		DSS04.05 Revisar, mantener y mejorar el plan de continuidad	Realizar una revisión por la Dirección de la capacidad de continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio.	
		DSS04.06 Proporcionar formación en el plan de continuidad	Proporcionar a todas las partes implicadas, internas y externas, de sesiones formativas regulares que contemplen los procedimientos y sus roles y responsabilidades en caso de disrupción.	
		DSS04.07 Gestionar acuerdos de respaldo	Mantener la disponibilidad de la información crítica del negocio.	
		DSS04.08 Ejecutar revisiones post reanudación	Evaluar la adecuación del Plan de Continuidad de Negocio (BCP) después de la reanudación exitosa de los procesos de negocio y servicios después de una disrupción.	
DSS05 Gestionar servicios de seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política deseguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	DSS05.01 Proteger contra software malicioso (malware)	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).	410-10 410-11
		DSS05.02 Gestionar la seguridad de la red y las conexiones	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.	
		DSS05.03 Gestionar la seguridad de los puestos de usuario final	Asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida.	
		DSS05.04 Gestionar la identidad del usuario y el acceso lógico	Asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con losrequerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio.	
		DSS05.05 Gestionar el acceso físico a los activos de TI	Definir e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendoemergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Esto aplicará a todas las personas que entren en los locales, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.	
		DSS05.06 Gestionar documentos sensibles y dispositivos de salida	Establecer salvaguardas físicas apropiadas, prácticas de contabilidad y gestión del inventario para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad.	
		DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad	Usando herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.	
		DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos	Evaluar y supervisar continuamente la ejecución de las actividades de los procesos de negocio y controlesrelacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio.	

DSS06 Gestionar controles de procesos de negocio	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.	DSS06.02 Controlar el procesamiento de la información	Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de lainformación es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado).	N/A
		DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe donde están los datos y quien los está manejando en su nombre.	
		DSS06.04 Gestionar errores y excepciones	Gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio.	
		DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información	Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.	
		DSS06.06 Asegurar los activos de información	Asegurar los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos activos en cualquier forma, dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda dela información de comienzo a fin.	
Monitorear, Evaluar y Valorar (MEA)				
MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	MEA01.01 Establecer un enfoque de la supervisión	Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.	N/A
		MEA01.02 Establecer los objetivos de cumplimiento y rendimiento	Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.	
		MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento	Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio.	
		MEA01.04 Analizar e informar sobre el rendimiento	Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión.	
		MEA01.05 Asegurar la implantación de medidas correctivas	Apoyar a las partes interesadas en la identificación,inicio y seguimiento de las acciones correctivas parasolventar anomalías.	
MEA02 Supervisar, evaluar y valorar el sistema de control interno	Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.	MEA02.01 Supervisar el control interno	Realizar, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos.	N/A
		MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio	Revisar la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Incluiractividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismoscomo la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centrosde operación de red. Esto proporciona al negocio de la seguridad de la efectividad del control para satisfacer los requisitos relativos al negocio y a las responsabilidades sociales y regulatorias.	
		MEA02.03 Realizar autoevaluaciones de control	Estimular a la Dirección y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Dirección sobre los procesos, políticas y contratos.	
		MEA02.04 Identificar y comunicar las deficiencias de control	Identificar deficiencias de control y analizar e identificarlas causas raíz subyacentes. Escalar las deficiencias decontrol y comunicarlas a las partes interesadas.	
		MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados	Asegurar que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance. Las entidades que realizan el aseguramiento deberían demostrar una actitud y apariencia apropiadas y adecuada competencia en las habilidades y conocimientos que son necesarios para realizar el aseguramiento y la adherencia a los códigos de ética y los estándares profesionales.	
		MEA02.06 Planificar iniciativas de aseguramiento	Planificar las iniciativas de aseguramiento basándoseen los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursosy suficiente conocimiento de la compañía.	
		MEA02.07 Estudiar las iniciativas de aseguramiento	Definir y acordar con la dirección el ámbito de la iniciativa de aseguramiento, basándose en los objetivosde aseguramiento.	

		MEA02.08 Ejecutar las iniciativas de aseguramiento	Ejecutar la iniciativa de aseguramiento planificada. Informar de los hallazgos identificados. Proveer opiniones de aseguramiento positivo, cuando sea oportuno, y recomendaciones de mejora relativas a los riesgos residuales identificados en el desempeño operacional, el cumplimiento externo y el sistema de control interno.	
MEA03 Supervisar, evaluar y valorar la conformidad con los requisitos externos	Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.	MEA03.01 Identificar requisitos externos de cumplimiento	Identificar y supervisar, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI.	N/A
		MEA03.02 Optimizar la respuesta a requisitos externos	Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar que estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse.	
		MEA03.03 Confirmar el cumplimiento de requisitos externos	Confirmar el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales.	
		MEA03.04 Obtener garantía de cumplimiento de requisitos externos	Obtener y notificar garantías de cumplimiento y adherencia a políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para tratar las diferencias en el cumplimiento son cerradas a tiempo.	

ANEXO 4:

VALORACIÓN PROCESOS

Cálculo de los valores para la herramienta

En este anexo se detalla el proceso realizado para obtener los valores que se ingresaron en la herramienta Self Assesment Template.

En cada nivel se evalúan criterios y según su cumplimiento se obtiene un porcentaje para el nivel, estos criterios están basados en COBIT.

Para evaluar los criterios se toma en cuenta las respuestas negativas y positivas como porcentaje, si existe un No, equivale a 0%, un Si, es 100%.

EDM01 ASEGURAR EL ESTABLECIMIENTO Y MANTENIMIENTO DEL MARCO DE REFERENCIA DE GOBIERNO

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	No
Existe evidencia del alcance del propósito del proceso.	No
Total	0

El nivel de este proceso es 0.

EDM03 ASEGURAR LA OPTIMIZACIÓN DEL RIESGO

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	No
Existe evidencia del alcance del propósito del proceso.	No
Total	0

El nivel de este proceso es 0.

EDM04 Asegurar la optimización de recursos

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	Si
Existe evidencia del alcance del propósito del proceso.	Si
Total	100
Nivel 1	
Criterio a evaluar	Se cumple
Las necesidades de recursos de la empresa son cubiertos con capacidades óptimas.	
Se conocen las necesidades de recursos de la empresa	Si
Existe realimentación de las partes interesadas sobre la optimización de los recursos	No

Existen beneficios (p.ej., ahorro de costes) que se logran a través de la utilización óptima de los recursos	Si
Se contabilizan las desviaciones del plan de recursos y las estrategias de arquitectura empresarial	No
Total	50
Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones.	
Se realiza un análisis de necesidades conjuntamente con Talento Humano y el área administrativa.	Si
Se asigna un presupuesto anual para abastecer las necesidades de recursos	Si
Se documenta la obtención y asignación de recursos	Si
Se analiza la asignación de recursos adecuados para los proyectos	Si
Los usuarios sienten que cuentan con los recursos apropiados	No
Total	80
El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico.	
Se reutilizan los componentes tecnológicos	Si
Se establecen políticas y principios para el cuidado de los recursos.	No
Se asignan responsables para asegurar el cuidado de los recursos	Si
Se realizan revisiones periódicas para el mantenimiento correcto de los recursos	Si
Existe un equipo de soluciones para los conflictos generados asociados a los recursos	Si
Total	80
Total	70
Nivel 2	
Criterio a evaluar	Se cumple
Se identifican los objetivos para el rendimiento del proceso	No
El rendimiento del proceso es planeado y monitoreado	No
El rendimiento del proceso es planeado	No
El rendimiento del proceso es monitoreado	No
El rendimiento de los procesos se ajusta para cumplir con los planes	No
Las responsabilidades y autoridades para el rendimiento del proceso son definidos, asignados y comunicados	50
Se han definido autoridades necesarios para el rendimiento del proceso	Si
Se han definido responsabilidades necesarios para el rendimiento del proceso	Si
Se han asignado las responsabilidades y autoridades	No
Se han comunicado las responsabilidades y autoridades	No
Los recursos y la información necesarios para el rendimiento del proceso son identificados, disponibilizados, localizados y usados	25
Se han identificado los recursos y la información necesarios para el rendimiento del proceso	SI
Se han disponibilizado los recursos y la información	No
Se han localizado los recursos y la información	No
Se han usado los recursos y la información	No

Las interfaces entre las partes envueltas se gestionan para asegurar comunicación efectiva y una clara asignación de responsabilidad.	No
Se han establecido medios de comunicación con las partes interesadas	No
Los requerimientos para los productos de trabajo del proceso son definidos.	No
Los requerimientos para documentación y control de los productos de trabajo son definidos.	No
Los productos de trabajo son apropiadamente identificados, documentados y controlados.	No
Los productos de trabajo identificados.	No
Los productos de trabajo son documentados.	No
Los productos de trabajo controlados.	No
Se han establecido controles para los productos de trabajo	No
Los productos de trabajo son revisados de acuerdo a los arreglos planeados y ajustados de acuerdo a la necesidad para cumplir con requerimientos.	No
Total	13

El nivel de este proceso es 2.

APO01 Gestionar el marco de gestión de TI

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	Si
Existe evidencia del alcance del propósito del proceso.	Si
Total	100
Nivel 1	
Criterio a evaluar	Se cumple
Un conjunto efectivo de políticas ha sido definido y mantenido.	
Se ha establecido un conjunto de políticas	Si
Se dan controles para mantener las políticas establecidas.	No
Total	50
Todos están al tanto de las políticas y como deberían ser implementadas	
Las políticas han sido socializadas con todos los empleados	No
Se han realizado planes sobre la implementación de las políticas.	No
Total	0
Total	25

El nivel de este proceso es 1.

APO02 Gestionar la estrategia

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	Si
Existe evidencia del alcance del propósito del proceso.	Si
Total	100
Nivel 1	
Criterio a evaluar	Se cumple

Todos los aspectos de la estrategia de TI están alineados con la estrategia del negocio	
Se conocen las necesidades de recursos de la empresa	Si
Existe realimentación de las partes interesadas sobre la optimización de los recursos	No
Existen beneficios (p.ej., ahorro de costes) que se logran a través de la utilización óptima de los recursos	Si
Se contabilizan las desviaciones del plan de recursos y las estrategias de arquitectura empresarial	No
Total	50
La estrategia de TI es coste-efectiva, apropiada, realista, factible, enfocada al negocio y equilibrada.	
Se realiza un análisis de necesidades conjuntamente con Talento Humano y el área administrativa.	Si
Se asigna un presupuesto anual para abastecer las necesidades de recursos	Si
Se documenta la obtención y asignación de recursos	Si
Se analiza la asignación de recursos adecuados para los proyectos	Si
Los usuarios sienten que cuentan con los recursos apropiados	No
Total	0
Se pueden derivar objetivos a corto plazo claros, concretos, y trazables de iniciativas a largo plazo específicas, y se pueden traducir, por tanto, en planes operativos	
Se reutilizan los componentes tecnológicos	Si
Se establecen políticas y principios para el cuidado de los recursos.	No
Se asignan responsables para asegurar el cuidado de los recursos	Si
Se realizan revisiones periódicas para el mantenimiento correcto de los recursos	Si
Existe un equipo de soluciones para los conflictos generados asociados a los recursos	Si
Total	20
TI es un generador de valor para el negocio.	
Se reutilizan los componentes tecnológicos	Si
Se establecen políticas y principios para el cuidado de los recursos.	No
Se asignan responsables para asegurar el cuidado de los recursos	Si
Se realizan revisiones periódicas para el mantenimiento correcto de los recursos	Si
Existe un equipo de soluciones para los conflictos generados asociados a los recursos	Si
Total	15
Total	22

APO07 Gestionar los recursos humano

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	No

Existe evidencia del alcance del propósito del proceso.	No
Total	0

El nivel de este proceso es 0.

AP012 Gestionar el riesgo

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	No
Existe evidencia del alcance del propósito del proceso.	No
Total	0

El nivel de este proceso es 0.

AP013 Gestionar la seguridad

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	No
Existe evidencia del alcance del propósito del proceso.	No
Total	0

El nivel de este proceso es 0.

BAI09 Gestionar los activos

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	Si
Existe evidencia del alcance del propósito del proceso.	Si
Total	100
Nivel 1	
Criterio a evaluar	Se cumple
Las licencias están alineadas a las necesidades del negocio	No
Los bienes se mantienen a niveles óptimos	
Se realizan análisis de activos utilizados y no utilizados	Si
Se realizan inventarios de los activos	Si
Se analizan los activos obsoletos	No
Se establecen políticas de uso de los activos	No
Se asignan responsables de los activos	Si
Se comunican a los usuarios y responsables los cuidados que se deben tener para prolonga la vida útil de los activos	No
Total	50
Total	25

El nivel de este proceso es 1.

DSS01 Gestionar operaciones

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	No
Existe evidencia del alcance del propósito del proceso.	No
Total	0

El nivel de este proceso es 0.

DSS04 Gestionar la continuidad

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	No
Existe evidencia del alcance del propósito del proceso.	No
Total	0

El nivel de este proceso es 0.

DSS05 Gestionar servicios de seguridad

Nivel 0	
Criterio a evaluar	Se cumple
El proceso se ha implementado o alcanza su objetivo.	Si
Existe evidencia del alcance del propósito del proceso.	Si
Total	100
Nivel 1	
Criterio a evaluar	Se cumple
La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio	
Se realizan análisis de de vulnerabilidades	No
Se implementan controles de seguridad de redes	Si
Se realizan pruebas para comprobar la efectividad de los mecanismos de seguridad	No
Las redes y comunicaciones son filtradas para evitar accesos a aplicaciones y sitios potencialmente peligrosos	Si
Total	50
La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	
Se han implementado seguridades en las terminales de usuario final	Si
El usuario final ha recibido capacitación sobre seguridad	No
Total	50
Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio	
Todos los usuarios están identificados y usan contraseñas seguras	Si

Todos usuarios conocen del manejo seguro de contraseñas	No
Los usuarios tienen acceso según su perfil de usuario	Si
Se analizan los datos de ingreso, ingreso fallido, número de intentos de inicio de sesión	No
Total	50
Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	
Se han implantado medidas físicas para proteger la información de accesos no autorizados	Si
Se realizan pruebas periódicas para evaluar la efectividad de estas herramientas	No
Total	50
La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida	No
Total	40

El nivel de este proceso es 1.

ANEXO 5:

RESULTADOS DE MSAT

Microsoft Security Assessment Tool
MTOP
Completado 17-jun-15 12:52

Informe completo

Este informe consta de las siguientes secciones:

Un socio de Microsoft puede revisar este informe con usted y ayudarle a elaborar un plan de acción detallado para poner en práctica las recomendaciones. Si aún no mantiene ninguna relación comercial con un socio de Microsoft, puede consultar una lista de socios de Microsoft para las soluciones de seguridad en https://solutionfinder.microsoft.com.

La herramienta Microsoft Security Assessment Tool se ha diseñado para ayudarle a determinar los riesgos a los que se enfrenta su infraestructura informática y las medidas que ha adoptado para combatirlos, además de sugerir medidas adicionales para contribuir aún más a la reducción del nivel de riesgos. No debe en ningún caso reemplazar a cualquier otra auditoría llevada a cabo por profesionales.

El uso de Microsoft Security Assessment Tool se rige por las condiciones del contrato de licencia que acompaña al software, y este informe está sujeto a las exclusiones, renuncias y limitaciones de responsabilidad que se incluyen en el contrato de licencia.

El propósito de este informe es meramente informativo. Ni Microsoft Corporation, ni sus proveedores o socios realizan o expresan implícitamente, ninguna declaración formal ni garantía alguna acerca de la herramienta Microsoft Security Assessment Tool, así como tampoco del uso, la precisión o la fiabilidad de los resultados de la evaluación e información que se incluye en este informe.

Resumen ejecutivo

Introducción

La herramienta Microsoft Security Assessment Tool se ha diseñado para ayudarle a identificar y abordar riesgos de seguridad en su entorno informático. Desde un enfoque holístico, se analiza la estrategia de seguridad al tratar distintos temas como el personal, los procesos y la tecnología. Los resultados se asocian con las soluciones recomendadas, incluyendo enlaces a más información de orientación adicional, en caso necesario. Estos recursos podrían ayudarle a asimilar más conceptos sobre las herramientas y los métodos específicos que puedan aumentar la seguridad de su entorno.

Esta sección de resumen pretende ofrecer a los responsables de TI y encargados senior una visión de los niveles de seguridad globales de la empresa. Puede consultar los resultados y las recomendaciones de forma detallada en el informe que le mostramos a continuación.

Historial del personal: Proceso y ámbito de autoevaluación

La evaluación se ha diseñado para identificar el riesgo comercial de su empresa y las medidas de seguridad utilizadas para mitigar dicho riesgo. A partir de los problemas más comunes del sector, se han desarrollado preguntas con las que es posible realizar una evaluación de alto nivel de las tecnologías, los procesos y el personal de la empresa.

La herramienta comienza con una serie de preguntas sobre el modelo de su empresa, para ir construyendo un perfil de riesgo para la empresa (BRP) mediante la valoración del riesgo al que su empresa está expuesta conforme al modelo y sector empresarial seleccionados. Se plantea una segunda serie de preguntas para compilar las medidas de seguridad que su empresa ha ido implantado a lo largo del tiempo. Todas juntas, esas medidas de seguridad forman capas de defensa, lo que proporciona una mayor protección frente a los riesgos de seguridad y las vulnerabilidades específicas. Cada capa contribuye a una estrategia combinada de defensa en profundidad. Esta suma se denomina Índice de defensa en profundidad (DiDI). A continuación, se comparan el BRP y el DiDI para medir la distribución de riesgos a lo largo de las áreas de análisis (AoAs): infraestructura, aplicaciones, operaciones y personal.

Además de centrarse en la correspondencia entre los riesgos de seguridad y las defensas, esta herramienta también valora la madurez de la seguridad en su empresa. La madurez de la seguridad hace referencia a la evolución hacia una mayor seguridad y prácticas sostenibles. En la escala inferior, se emplean pocas defensas de seguridad y las acciones son reactivas. En el lado opuesto, los procesos establecidos y probados permiten a la empresa ser más proactiva, además de responder de forma más eficaz y sistemática cuando es necesario.

En este contexto, a partir de las tecnologías, los aspectos de seguridad y las estrategias de defensa en profundidad existentes, se ofrecen sugerencias sobre la gestión de riesgos para los entornos específicos. Estas sugerencias tienen como fin conducirle a buen ritmo hacia la consecución de las mejores prácticas para su caso particular.

La presente evaluación, incluidas las preguntas, medidas y recomendaciones, está diseñada para empresas medianas que tengan entre 50 y 500 equipos de escritorio. Su objetivo es estudiar de forma general las áreas de riesgos potenciales, en lugar de proporcionar un análisis en profundidad de una tecnología o un proceso concretos. Como resultado, la herramienta no puede medir la eficacia de las medidas de seguridad utilizadas. Con este fin, la información que recibe debe servirle de guía preliminar para centrarse en las áreas específicas que exigen una atención más rigurosa y no debe en ningún caso reemplazar a cualquier otra evaluación específica realizada por equipos de evaluación independientes cualificados.

Análisis de la situación

Este gráfico de la sección representa los conceptos de su empresa descritos anteriormente y se basa en las respuestas que proporcionó. Recuerde:

- BRP es una medición del riesgo relacionado al modelo empresarial y al sector de la empresa
- DiDI es una medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en una empresa.
- La madurez de la seguridad es una medición de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de diversas disciplinas.

[Consulte los apéndices para obtener información adicional acerca de estos términos y cómo interpretar los gráficos.]

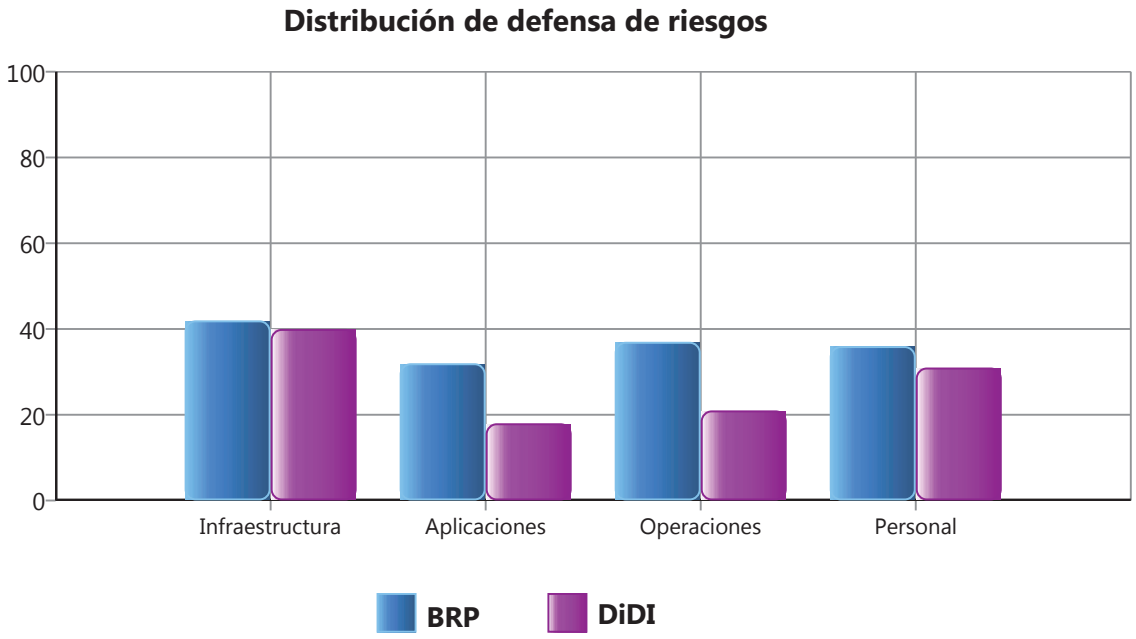
Resultados:

Áreas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Personal		
Operaciones		
Aplicaciones		

Infraestructura

Distribución de defensa de riesgos

Este gráfico, dividido en áreas de análisis, muestra las diferencias en el resultado de la defensa en profundidad.



Por lo general, es mejor contar con una calificación de DiDI del mismo nivel que otra de BRP para la misma categoría. Un desequilibrio, ya sea dentro de una categoría o entre categorías, en cualquier dirección, puede indicar la necesidad de volver a alinear sus inversiones de TI.

Madurez de la seguridad

La madurez de la seguridad incluye los controles (tanto físicos como técnicos), la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. Debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centrar los programas de seguridad de la empresa. No todas las empresas deben esforzarse por alcanzar el nivel óptimo, pero todas deben evaluar en qué punto se encuentran y determinar el lugar que deberían ocupar en vista de los riesgos comerciales a los que se enfrentan. Por ejemplo, puede que una empresa con un entorno de bajo riesgo no necesite nunca subir encima del límite superior del nivel básico o el límite inferior del nivel estándar. Las empresas con un entorno de alto riesgo probablemente entren de lleno en el nivel optimizado. Los resultados del perfil de riesgos para la empresa le permiten hacer un balance de los riesgos.

Madurez de la seguridad	Una medida de las prácticas de una empresa con respecto a las mejores prácticas de la industria para la seguridad sostenible. Todas las empresas deben esforzarse en alinear su nivel de madurez y estrategia de seguridad asociada, en relación a los riesgos que conlleva su actividad comercial:
Básica	Algunas medidas eficaces de seguridad utilizadas como primer escudo protector; respuesta de operaciones e incidentes aún muy reactiva
Estándar	Capas múltiples de defensa utilizadas para respaldar una estrategia definida
Optimizada	Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas

Tarjeta de puntuación

De acuerdo con sus respuestas acerca de la evaluación de riesgos, sus medidas de defensa se han calificado de la siguiente forma. Las secciones Detalles de la evaluación y Lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Leyenda: ● Cumple las mejores prácticas recomendadas ● Necesita mejorar ● Carencias severas

Infraestructura	●
Defensa del perímetro	●
Reglas y filtros de cortafuegos	●
Antivirus	●
Antivirus - Equipos de escritorio	●
Antivirus - Servidores	●
Acceso remoto	●
Segmentación	●
Sistema de detección de intrusiones (IDS)	●
Inalámbrico	●
Autenticación	●
Usuarios administrativos	●
Usuarios internos	●
Usuarios de acceso remoto	●
Directivas de contraseñas	●
Directivas de contraseñas-Cuenta de administrador	●
Directivas de contraseñas-Cuenta de usuario	●
Directivas de contraseñas-Cuenta de acceso remoto	●
Cuentas inactivas	●
Gestión y control	●
Informes sobre incidentes y respuesta	●
Creación segura	●
Seguridad física	●

Aplicaciones	●
Implementación y uso	●
Equilibrio de carga	●
Clústeres	●
Aplicación y recuperación de datos	●
Fabricante de software independiente (ISV)	●
Desarrollado internamente	●

Operaciones	●
Entorno	●
Host de gestión	●
Host de gestión-Servidores	●
Host de gestión - Dispositivos de red	●
Directiva de seguridad	●
Clasificación de datos	●
Eliminación de datos	●
Protocolos y servicios	●
Uso aceptable	●
Gestión de cuentas de usuarios	●
Regulación	●
Directiva de seguridad	●
Gestión de actualizaciones y revisiones	●
Documentación de la red	●
Flujo de datos de la aplicación	●
Gestión de actualizaciones	●
Gestión de cambios y configuración	●
Copias de seguridad y recuperación	●
Archivos de registro	●
Planificación de recuperación ante desastres y reanudación de negocio	●
Copias de seguridad	●
Dispositivos de copia de seguridad	●
Copias de seguridad y restauración	●

Personal	●
Requisitos y evaluaciones	●
Requisitos de seguridad	●
Evaluaciones de seguridad	●
Directiva y procedimientos	●

Vulnerabilidades	🔴
Diseño de aplicaciones	🔴
Autenticación	🔴
Directivas de contraseñas	🔴
Autorización y control de acceso	🟢
Registro	🟢
Validación de datos de entrada	🔴
Metodologías de desarrollo de seguridad de software	🔴
Almacenamiento y comunicaciones de datos	🔴
Cifrado	🔴
Cifrado - Algoritmo	🔴

Comprobaciones del historial personal	🟢
Directiva de recursos humanos	🔴
Relaciones con terceros	🔴
Formación y conocimiento	🔴
Conocimiento de seguridad	🟡
Formación sobre seguridad	🔴

Iniciativas de seguridad

Las siguientes áreas no cumplen las mejores prácticas recomendadas y deben dirigirse a aumentar la seguridad de su entorno. Las secciones Detalles de la evaluación y Lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Prioridad alta	Prioridad intermedia	Prioridad baja
• Usuarios de acceso remoto • Acceso remoto • Segmentación • Creación segura • Relaciones con terceros	• Seguridad física • Inalámbrico • Conocimiento de seguridad • Reglas y filtros de cortafuegos • Cuentas inactivas	• Antivirus - Equipos de escritorio • Antivirus - Servidores • Autorización y control de acceso • Regulación • Directiva de seguridad

Evaluación detallada

Esta sección del informe ofrece los resultados detallados para cada categoría, así como las mejores prácticas, recomendaciones y referencias de información adicional. Las recomendaciones son prioritarias en la siguiente sección.

Áreas de análisis

La siguiente tabla enumera las áreas incluidas para el análisis de alto nivel de esta evaluación de riesgos para la seguridad y explica la relación entre cada área y la seguridad. La sección "Detalles de la evaluación" describe los niveles de seguridad de su empresa (según las respuestas aportadas en la evaluación) con respecto a cada una de estas áreas. Asimismo, indica las prácticas más reconocidas del sector, además de ofrecerle recomendaciones para implantar tales prácticas.

Categoría	Importancia para la seguridad
Perfil de riesgos para la empresa (BRP)	
Perfil de riesgos para la empresa (BRP)	Comprender como la propia naturaleza de la empresa afecta a los riesgos es importante a la hora de decidir dónde aplicar los

	recursos que ayuden a paliar tales riesgos. El reconocimiento de las áreas le permitirá optimizar la asignación del presupuesto de seguridad.
Infraestructura	
Defensa del perímetro	La defensa del perímetro trata la seguridad del perímetro de la red, donde su red interna conecta con el exterior. Este es su primer escudo protector contra los intrusos.
Autenticación	Los procedimientos estrictos de autenticación de usuarios, administradores y usuarios remotos ayudan a asegurar que los intrusos no accedan sin autorización a la red mediante ataques locales o remotos.
Gestión y control	La gestión, supervisión y el registro adecuados son elementos vitales para mantener y analizar los entornos informáticos. Estas herramientas son aún más importantes después de un ataque, cuando se necesita un análisis del incidente.
Aplicaciones	
Implantación y utilización	Cuando se implantan aplicaciones críticas para la empresa, hay que asegurar la seguridad y la disponibilidad de esas aplicaciones y de los servidores. El mantenimiento continuo es imprescindible para ayudarle a asegurarse de que los errores de seguridad se corrigen y que no se introducen nuevas vulnerabilidades en el entorno.
Diseño de aplicaciones	Un diseño que no aborda adecuadamente los mecanismos de seguridad como la autenticación, la autorización, y la validación de datos podría permitir que los atacantes aprovechen las vulnerabilidades de seguridad para acceder a información confidencial.
Almacenamiento y comunicaciones de datos	La integridad y confidencialidad de los datos son dos de las prioridades que debe garantizar cualquier empresa. La pérdida o el robo de datos puede afectar negativamente tanto a los ingresos de una entidad como a su reputación. Es importante comprender como las aplicaciones controlan y protegen los datos críticos.
Operaciones	
Entorno	La seguridad de una empresa depende de los procedimientos operativos, los procesos y las pautas que se aplican en el entorno. Pueden aumentar la seguridad incluyendo más que meras defensas tecnológicas. La capacidad del equipo de operaciones para mantener la seguridad del entorno depende de forma crucial de la documentación exacta del entorno y de las pautas.
Directiva de seguridad	La política de seguridad corporativa hace referencia a las directivas y a pautas individuales para regular el uso adecuado y seguro de las tecnologías y los procesos de la empresa. Esta área incluye las directivas para todos los aspectos de la seguridad, como los usuarios, los sistemas y los datos.
Gestión de actualizaciones y revisiones	La gestión adecuada de actualizaciones y revisiones es un factor importante para la seguridad del entorno informático de las empresas. La aplicación oportuna de actualizaciones y revisiones es necesaria para contribuir a la protección del entorno contra las vulnerabilidades conocidas y aquellas que podrían ser un frente de ataque.
Copias de seguridad y recuperación	Las copias de seguridad y la recuperación de datos son imprescindibles para el mantenimiento de la continuidad de los servicios comerciales en caso de un accidente o fallo de hardware

	o de software. La falta de procedimientos adecuados para realizar copias de seguridad y recuperación podría producir una pérdida significativa de datos y de productividad.
Personal	
Requisitos y evaluaciones	Todos los encargados de la toma de decisiones deben comprender los requisitos de seguridad para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad, en lugar de contradecirse entre sí. Las evaluaciones periódicas realizados por terceros independientes pueden ayudar a la empresa a revisar, evaluar e identificar las posibles mejoras.
Directivas y procedimientos	Los procedimientos claros y prácticos en la gestión de las relaciones con los fabricantes y socios pueden ayudarle a minimizar el nivel de riesgos al que se expone la empresa. Los procedimientos para contratar aspirantes y finalizar sus contratos pueden proteger a la empresa contra empleados sin escrúpulos o descontentos.
Formación y conocimiento	Los empleados deben recibir formación para que sean conscientes de cómo las medidas de seguridad afectan a sus actividades diarias, para que no expongan a la empresa a mayores riegos de forma inadvertida.

Análisis de la evaluación

Esta sección está dividida en las cuatro principales áreas de análisis: infraestructura, aplicaciones, operaciones y personal.

Infraestructura

La seguridad de las infraestructuras se centra en cómo debe funcionar la red, los procesos comerciales (internos o externos) que se deben implantar, cómo se crean y utilizan los hosts y la gestión y el mantenimiento de la red. La seguridad de la infraestructura efectiva puede ayudarle a mejorar significativamente la defensa de la red, las reacciones a incidentes, la disponibilidad de la red y el análisis de fallos. Al establecer un diseño de la infraestructura que todos puedan comprender y seguir, podrá identificar las áreas de riesgo y desarrollar métodos para reducir las amenazas. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar el riesgo para la infraestructura enfocándose en las áreas de seguridad de infraestructura que siguen:

- Defensa del perímetro—cortafuegos, antivirus, acceso remoto, segmentación
- Autentificación—directivas de contraseñas
- Gestión y control—hosts de gestión, archivos de registro
- Estación de trabajo—configuración de creación

Defensa del perímetro	
Subcategoría	**Mejores prácticas recomendadas**
Reglas y filtros de cortafuegos	Los firewalls son un mecanismo de primera línea de defensa y se deben colocar en todas las ubicaciones de borde de red. Las reglas implementadas en los firewalls deben ser muy restrictivas y establecerse host a host y servicio a servicio. Al crear reglas de firewall y listas de control de acceso (ACL) de enrutador, céntrese primero en la protección de los dispositivos de control y de la red frente a ataques. El firewall debe estar establecido con una posición de denegación predeterminada, permitiendo únicamente el tráfico necesario.

	* Aplique el flujo de datos utilizando las ACL de red y las reglas de firewall. * Pruebe las reglas de firewall y ACL de enrutador para determinar si las reglas existentes contribuyen a ataques de denegación de servicio (DoS). * Implemente una o más DMZ como parte de una implementación de firewall sistemática y formal. * Coloque ahí todos los servidores accesibles a través de Internet. Restrinja la conectividad hacia las DMZ y desde ellas.	
	Resultados	**Recomendaciones**
Reglas y filtros de cortafuegos	Sus respuestas indican que ha instalado cortafuegos en todas las oficinas.	Continúe implementando cortafuegos u otros controles de acceso de nivel de red en todas las ubicaciones de oficinas, realice pruebas con frecuencia y verifique que todos los cortafuegos funcionan correctamente.
Reglas y filtros de cortafuegos	Sus respuestas indican que utiliza software de cortafuegos basados en hosts para proteger los servidores.	Continúe instalando cortafuegos basados en host en todos los servidores y piense también en emplear este software en todos los equipos de escritorio y portátiles en la empresa.
Reglas y filtros de cortafuegos	Sus respuestas indican que, aunque ha dado el primer paso para proteger el perímetro de la red con un cortafuegos, no ha creado ningún segmento DMZ para proteger los recursos corporativos a los que se puede acceder a través de Internet desde los dispositivos internos de la empresa.	Estudie la utilización de un cortafuegos para separar los recursos accesibles por Internet, como servidores Web, de los recursos internos y corporativos. Ponga en práctica reglas que controlen el acceso de entrada y salida. Plantéese la utilización de filtros de salida para evitar conexiones innecesarias y limitar el acceso directo a los segmentos DMA por parte de los usuarios internos, ya que no es probable que éstos trabajen con los equipos hosts del DMZ con frecuencia. Limite el acceso de la red central al segmento DMZ sólo a hosts específicos o a redes administrativas.
Reglas y filtros de cortafuegos	Sus respuestas indican que el cortafuegos no se comprueba regularmente para asegurarse de que funciona correctamente.	Establezca pruebas periódicas del cortafuegos. Asegúrese de que la funcionalidad responde según lo previsto, no únicamente desde el tráfico externo, y compruebe que el cortafuegos también está respondiendo al tráfico interno.
Subcategoría	**Mejores prácticas recomendadas**	
Antivirus	Implemente soluciones antivirus en todo el entorno en el nivel de servidor y de escritorio. Implemente soluciones antivirus especializadas para tareas específicas, como exploradores de servidores de archivos, herramientas de filtrado de contenido y exploradores de carga y descarga de datos. Configure soluciones antivirus para buscar virus en el entorno tanto de entrada como de salida. Las soluciones antivirus se deben implementar primero en servidores de archivos críticos y, a continuación, en servidores de correo, bases de datos y web. La solución antivirus se debe incluir en el entorno de generación predeterminado para escritorios y portátiles. Si utiliza Microsoft Exchange, utilice las capacidades de antivirus y filtrado de contenido	

	adicionales en el nivel de buzón.

Subcategoría	Mejores prácticas recomendadas	
Antivirus - Equipos de escritorio		
	Resultados	**Recomendaciones**
Antivirus - Equipos de escritorio	Su respuesta indica que los equipos de escritorio utilizan soluciones antivirus.	Continúe con la práctica. Utilice una directiva que requiera a los usuarios a actualizar las firmas de virus. Piense en añadir el cliente antivirus al entorno predeterminado de creación de estaciones de trabajo.

Subcategoría	Mejores prácticas recomendadas	
Antivirus - Servidores		
	Resultados	**Recomendaciones**
Antivirus - Servidores	Sus respuestas indican que ha utilizado soluciones antivirus en el nivel del servidor.	Continúe con la práctica. Plantéese controlar activamente los clientes antivirus de los servidores desde una consola de gestión central para la utilización de configuraciones y firmas de virus. Si utiliza Microsoft Exchange, considere emplear las funciones adicionales de antivirus y los filtros de contenidos para los buzones de correo.

Subcategoría	Mejores prácticas recomendadas	
Acceso remoto	Es importante seguir un proceso de creación de informes de incidentes y repuesta documentado para garantizar que todos los problemas e incidentes se revisan y se evalúan de forma coherente. Es importante que todos los usuarios comprendan su responsabilidad de notificar los problemas o incidentes de seguridad y que tengan un proceso definido claramente para notificar estos problemas.	
	Resultados	**Recomendaciones**
Acceso remoto	Sus respuestas indican que existen empleados y/o socios que se conectan remotamente a la red interna, pero no utiliza ninguna tecnología VPN para permitirles un acceso seguro.	Utilice VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH. Utilice conectividad sitio-a-sitio basada en la tecnología IPSec. Configure listas de acceso a redes y de usuario para limitar el acceso a los recursos corporativos necesarios.
Acceso remoto	Sus respuestas indican que existen empleados y/o socios que se conectan remotamente a la red interna y que ha dado el paso importante de utilizar tecnología VPN para permitirles el acceso.	Estudie utilizar la autenticación multifactor para la conexión de usuarios remotos a través de Internet a los recursos corporativos. Revise con regularidad la lista de acceso de los usuarios en el

	Sin embargo, no ha utilizado autenticación multifactor como un segundo escudo protector.	dispositivo VPN.

Subcategoría	Mejores prácticas recomendadas
Segmentación	Utilice segmentos para impedir el acceso a extranets específicas por parte de fabricantes, socios o clientes. Cada segmento externo de la red debe permitir que sólo se encamine determinado tráfico hacia los hosts y puertos concretos de aplicaciones que proporcionan servicios a los clientes. Asegúrese de que existan controles de red que permitan sólo el acceso necesario para cada conexión de terceros. Limite el acceso de los servicios de red suministrados, así como el acceso entre los segmentos de red.

	Resultados	Recomendaciones
Segmentación	Sus respuestas indican que la red presenta más de un segmento.	Continúe empleando la segmentación de la red para mejorar la gestión del tráfico de la red y limitar el acceso a los recursos que se basan en los requisitos del usuario.
Segmentación	Su respuesta indica que los servicios ofrecidos en Internet no se alojan en la red de su empresa.	Si los servicios de Internet se exponen a otros servicios que van a albergarse en la red de la empresa, asegúrese de que los cortafuegos, la segmentación y los sistemas de detección de intrusiones protegen la infraestructura de la empresa de los ataques desde Internet.
Segmentación	Su respuesta indica que actualmente no existe segmentación de la red en el entorno. Es importante mantener los servicios extranet de clientes y socios en sus segmentos de red propios.	Traslade los servidores de acceso extranet a un segmento de red físicamente diferente. Aplique controles de acceso restrictivos para limitar el acceso de terceros a determinados hosts y a la infraestructura corporativa necesaria, además de bloquear los intentos de conexión con redes remotas.

Subcategoría	Mejores prácticas recomendadas
Sistema de detección de intrusiones (IDS)	Los sistemas de detección de intrusiones basados en host y en red deben implantarse para detectar y notificar cualquier ataque que se produzca contra los sistemas corporativos.

	Resultados	Recomendaciones
Sistema de detección de intrusiones (IDS)	Sus respuestas indican que no utiliza ningún hardware ni software de detección de intrusiones.	Considere la implantación de sistemas de detección de intrusiones basados en red o en host.

Subcategoría	Mejores prácticas recomendadas

Inalámbrico	Las mejores prácticas para la implantación inalámbrica incluyen la garantía de que la red no hace público su SSID, que se usa el cifrado WPA y que la red no se considera fundamentalmente como de no confianza.	
	Resultados	**Recomendaciones**
Inalámbrico	Sus respuestas indican que existe la opción de conexión inalámbrica a su red	Para reducir los riesgos asociados a las redes inalámbricas, la implantación no debe incluir la difusión del SSID, pero sí el cifrado WPA, además de tratar la red como de no confianza.
Inalámbrico	Su respuesta indica que ha modificado el SSID predeterminado del punto de acceso.	El cambio del SSID predeterminado es el primer paso para asegurar su red inalámbrica. No obstante, es necesario combinarlo con otras prácticas para minimizar el riesgo. Estas prácticas incluyen la no difusión del SSID, el cifrado WPA y tratar la red como de no confianza.
Inalámbrico	Sus respuestas indican que no ha desactivado la difusión del SSID en el punto de acceso.	Considere la deshabilitación de la difusión del SSID para dificultar a un usuario ocasional los intentos de conexión a su red inalámbrica.
Inalámbrico	Sus respuestas indican que no utiliza el cifrado WEP en el entorno inalámbrico.	Si actualmente no está utilizando ningún cifrado, considere utilizar WPA para evitar que el tráfico de la red inalámbrica sea "detectado" y leído como texto sin formato.
Inalámbrico	Sus respuestas indican que utiliza el cifrado WPA en el entorno inalámbrico.	En la actualidad, WPA es el estándar de cifrado más seguro pero aún se puede descodificar. Considere la utilización de un cifrado adicional (como VPN) para una mayor seguridad.
Inalámbrico	Sus respuestas indican que utiliza la restricción por MAC en el entorno inalámbrico.	La limitación de la dirección MAC ayuda a evitar que ordenadores no autorizados se conecten a la red, aunque este sistema de cifrado se puede descodificar de forma relativamente sencilla. Considere el uso de autenticación WPA además de los filtros MAC.
Inalámbrico	Sus respuestas indican que la red inalámbrica se considera de no confianza.	Considere migrar su red inalámbrica a un segmento de red de no confianza y exigir el uso de VPN o tecnologías similares para proteger mejor la integridad de los datos.

Defensa del perímetro - Recursos		
Windows Server 2008	Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply	http://www.microsoft.com/windowsserver2008/en/us/overview.aspx

	with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations.	
Internet Security and Acceleration Server	Internet Security and Acceleration (ISA) Server 2006 is the integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users with fast and secure remote access to applications and data.Deploy ISA Server 2006 for Secure Remote Access, Branch Office Security, and Internet Access Protection.	http://www.microsoft.com/forefront/edgesecurity/default.mspx
Intelligent Application Gateway	Microsoft's Intelligent Application Gateway (IAG) 2007 is the comprehensive, secure remote access gateway that provides secure socket layer (SSL)-based application access and protection with endpoint security management. IAG 2007 enables granular access control, authorization, and deep content inspection from a broad range of devices and locations to a wide variety of line-of-business, intranet, and client/server resources.	http://www.microsoft.com/forefront/edgesecurity/iag/default.mspx
Network Access Protection	Network Access Protection (NAP) is a new platform and solution that controls access to network resources based on a client computer identity and compliance with corporate governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.	http://technet.microsoft.com/en-us/network/bb545879.aspx

Autenticación	
Subcategoría	**Mejores prácticas recomendadas**
Usuarios administrativos	Ponga en práctica una directiva de contraseñas complejas para las cuentas administrativas con contraseñas que cumplan estas condiciones: + Alfanumérico + Mayúsculas y minúsculas + Contiene al menos un carácter especial

+ Contiene como mínimo 14 caracteres

Para limitar más los riesgos de ataques a las contraseñas, ponga en práctica los controles siguientes:

+ Caducidad de contraseñas
+ Bloqueo de la cuenta después de entre 7 y 10 intentos de registro fallidos
+ Registro del sistema

Además de las contraseñas complejas, puede recurrir a la autenticación multifactor. Utilice controles avanzados de la gestión de cuentas y del registro de acceso a cuentas (no permita que se compartan cuentas).

	Resultados	Recomendaciones
Usuarios administrativos	Sus respuestas indican que se utilizan inicios de sesión distintos para la administración de seguridad de los sistemas y de los dispositivos del entorno.	Continúe exigiendo cuentas separadas para las actividades administrativas o de gestión y asegúrese de que las credenciales administrativas se modifican con frecuencia.
Usuarios administrativos	Sus respuestas indican que los usuarios no tienen habilitados accesos administrativos a sus estaciones de trabajo.	Continúe sin permitir el acceso administrativo para los usuarios finales en sus estaciones de trabajo y asegúrese de que las credenciales administrativas para los mismos se cambian con frecuencia.

Subcategoría	Mejores prácticas recomendadas
Usuarios internos	Para las cuentas de usuario, implemente una directiva que requiera el uso de contraseñas complejas que cumplan los siguientes criterios: * Caracteres alfanuméricos * Uso de mayúsculas y minúsculas * Al menos un carácter especial * Longitud mínima de 8 caracteres Para limitar aún más el riesgo de un ataque a contraseñas, implemente los siguientes controles: * Caducidad de contraseña * Bloqueo de cuenta tras al menos 10 intentos de inicio de sesión erróneos * Registro del sistema Además de contraseñas complejas, considere la posibilidad de implementar una autenticación de varias fases. Implemente controles avanzados para la gestión de cuentas (no permita el uso compartido de cuentas) y para el registro de acceso a cuentas.

Subcategoría	Mejores prácticas recomendadas
Usuarios de acceso remoto	Implemente controles de contraseña complejos para todos los usuarios de acceso remoto, si se ha concedido este acceso mediante el uso de tecnologías de acceso telefónico o VPN. Una contraseña se considera compleja si cumple los siguientes criterios: * Caracteres alfanuméricos * Uso de mayúsculas y minúsculas * Al menos un carácter especial * Longitud mínima de 8 caracteres Implemente una fase adicional de autenticación para las cuentas a las que se ha concedido acceso remoto. Considere también la posibilidad de implementar controles avanzados para la gestión de cuentas (no permita el uso compartido de cuentas) y para

	el registro de acceso a cuentas. En el caso del acceso remoto, resulta especialmente importante proteger el entorno mediante el uso de unas prácticas de gestión de cuentas segura, buenas prácticas de registro y capacidades de detección de incidentes. Para mitigar aún más los riesgos de ataques de fuerza bruta a contraseñas, considere la posibilidad de implementar los siguientes controles: * Caducidad de contraseña * Bloqueo de cuenta tras 7 a 10 intentos de inicio de sesión erróneos * Registro del sistema Los servicios de acceso remoto también deben tener en cuenta los sistemas que se utilizan para obtener acceso a redes o hosts. Considere también la posibilidad de implementar controles para hosts a los que se les permite acceder a la red de forma remota.	
	Resultados	**Recomendaciones**
Usuarios de acceso remoto	Sus respuestas indican que los empleados pueden conectarse a la red de forma remota.	Si aún no lo ha hecho, estudie la utilización de un sistema de autenticación multifactor de acceso remoto y limite el acceso únicamente a aquellos empleados que tengan una necesidad empresarial de conectividad remota.
Usuarios de acceso remoto	Sus respuestas indican que los contratistas pueden conectarse a la red de forma remota.	Además de permitir el acceso remoto a los empleados según las mejores prácticas recomendadas, considere limitar el acceso a los contratistas para que únicamente puedan acceder a los sistemas remotos necesarios. Por otro lado, plantéese utilizar un punto de entrada separado para los contratistas, con el fin de controlar y limitar su acceso con más facilidad.
Usuarios de acceso remoto	Sus respuestas indican que terceros usuarios pueden conectarse a la red de forma remota.	Además de permitir el acceso remoto a los empleados según las mejores prácticas recomendadas, considere limitar el acceso a terceros para que únicamente puedan acceder a los sistemas remotos necesarios. Por otro lado, plantéese utilizar un punto de entrada separado para los terceros, con el fin de controlar y limitar su acceso con más facilidad.
Subcategoría	**Mejores prácticas recomendadas**	
Directivas de contraseñas	La utilización de contraseñas complejas es un elemento fundamental del índice de defensa en profundidad. Las contraseñas complejas deben tener de 8 a 14 caracteres e incluir caracteres alfanuméricos y especiales. Debe establecer una longitud mínima, un historial, un límite a la duración y una caducidad para reforzar la defensa. Generalmente, la caducidad de las contraseñas debe configurarse de esta forma: + Duración máxima de 90 días + Las cuentas nuevas deben cambiar la contraseña al inicio de la sesión + Un historial de 8 contraseñas (mínimo de 8 días) Además de las contraseñas complejas, la autenticación multifactor es muy importante, especialmente para las cuentas administrativas y de usuarios remotos.	

	En todas las cuentas de usuario, se debe activar un proceso de bloqueo de cuenta tras 10 intentos de registro fallidos. Los controles para bloquear una cuenta pueden variar; algunos sencillamente se dedican a los ataques de fuerza bruta a las contraseñas y otros requieren que un administrador desbloquee la cuenta. Se considera una práctica aconsejable activar el bloqueo en las cuentas administrativas, al menos en lo que respecta al acceso a la red. De esta forma, la cuenta no se puede bloquear desde fuera de la consola, solamente desde la red. Es posible que esta solución no sea adecuada para todas las empresas, particularmente para aquellas con ubicaciones remotas. En tales casos, lo más adecuado es que un administrador desbloquee la cuenta, de este modo se evita que los ataques pasen desapercibidos durante largo tiempo si no se dispone de otros medios para detectar fallos de autenticación. Cuando se pongan en práctica controles de bloqueo de cuenta, siga las normas siguientes: + Bloqueo después de entre 7 y 10 intentos de registro fallidos para las cuentas administrativas y de acceso remoto + Bloqueo después de 10 intentos de registro fallidos para las cuentas de usuario estándar + Requerir la intervención de un administrador para desbloquear las cuentas de acceso remoto y de administrador, y para reactivar automáticamente las cuentas de usuarios estándar al cabo de 5 minutos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las que se aplican a las cuentas normales. En sistemas Windows, debe establecer contraseñas de 14 caracteres alfanuméricos y especiales para las cuentas administrativas (y las cuentas de servicio).

	Resultados	**Recomendaciones**
Directivas de contraseñas	Sus respuestas indican que no existen controles formales para hacer cumplir las directivas de contraseñas en todas las cuentas.	Piense en implantar el uso de contraseñas complejas para todas las cuentas como en la sección de mejores prácticas recomendadas. Piense en implantar el uso de la caducidad de contraseñas como en la sección de mejores prácticas recomendadas.

Subcategoría	**Mejores prácticas recomendadas**
Directivas de contraseñas-Cuenta de administrador	

Subcategoría	**Mejores prácticas recomendadas**
Directivas de contraseñas-Cuenta de usuario	

Subcategoría	**Mejores prácticas recomendadas**
Directivas de contraseñas-Cuenta de acceso remoto	

Subcategoría	**Mejores prácticas recomendadas**

Cuentas inactivas	Continúe supervisando y gestionando cuentas inactivas. Establezca un proceso para incluir un procedimiento de notificación inmediata a todos los administradores del sistema para el personal que ya no está en la organización con el objeto de garantizar que sus cuentas se deshabiliten inmediatamente, especialmente sus cuentas de acceso remoto. Considere la posibilidad de implementar un proceso para revisar las cuentas actuales del personal que se transfiere a otro departamento dentro de la organización. Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información. Visite habitualmente los sitios de los fabricantes para obtener actualizaciones de las firmas de virus y descárguelas en un sitio aislado para probarlas en un entorno de laboratorio. Verifique que las actualizaciones no causen problemas con ningún sistema operativo ni aplicaciones antes de utilizarlas. Debe desactivar las funciones de actualización automática de las soluciones antivirus en todos los sistemas para evitar la utilización de archivos potencialmente peligrosos antes de su comprobación. Utilice una consola central para las aplicaciones antivirus, esta consola proporcionará información acerca de los sistemas obsoletos o con funciones de software desactivadas . Para los usuarios remotos que no se conectan regularmente a la red corporativa, puede usar la función de actualización automática. Las cuentas del personal que ya no está en la organización se deben deshabilitar a tiempo para garantizar que los usuarios eliminados u otros usuarios no puedan utilizar la cuenta para obtener acceso no autorizado. Si los administradores de sistemas no tienen información sobre los cambios del estado de un usuario debido a su transferencia, no cambiarán o quitarán los accesos al sistema o físicos. Esto puede dar lugar a un acceso no autorizado o excesivo por parte de los usuarios transferidos.

	Resultados	**Recomendaciones**
Cuentas inactivas	Su respuesta indica que existen directivas para las actualizaciones de firmas de virus en el entorno.	Visite con regularidad los sitios de fabricantes y otros proveedores de soluciones de seguridad para buscar avisos de ataques recientes y brotes de virus Realice auditorías regularmente para comprobar que los usuarios remotos actualizan sus sistemas. Trabaje conforme a las mejores prácticas recomendadas.
Cuentas inactivas	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información.

Autenticación - Recursos		
Windows Server 2008	Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that	http://www.microsoft.com/windowsserver2008/en/us/overview.aspx

	try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations.	
Windows Server Active Directory	A central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. Windows Server 2003 makes Active Directory simpler to manage, easing migration and deployment. Windows Server Active Directory is already used by companies around the world to gain unified management of identities and resources across the enterprise network. Active Directory enables organizations to centrally manage and track information about users and their privileges. In addition, Active Directory Lightweight Directory Services (ADLDS), an LDAP directory service, provides organizations with flexible support for directory-enabled applications. Integration with Microsoft Federated Identity, Strong Authentication, Information Protection and Identity Lifecycle Management solutions, makes Active Directory an ideal foundation for building a comprehensive identity and access solution.	http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx http://www.microsoft.com/windowsserver2003/technologies/idm/DirectoryServices.mspx
Windows Server Group Policy	Group Policy provides an infrastructure for centralized configuation management for the operating system and applications that run oh the operating system. Group Policy is supported in both Windows Server 2003 and has advanced features in Windows Server 2008 to extend the current configuration capabilites.	http://technet2.microsoft.com/windowsserver2008/en/library/3b4568bc-9d3c-4477-807d-2ea149ff06491033.mspx?mfr=true
Windows Server 2003 - Internet Authenication Services (IAS)	Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2003. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication	http://technet.microsoft.com/en-us/network/bb643123.aspx

	and accounting messages to other RADIUS servers. In Windows Server 2008, IAS has been replaced with Network Policy Server (NPS).	
Windows Server 2008 - Network Policy Server (NPS)	Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in Windows Server 2008. NPS is the replacement for Internet Authentication Service (IAS) in Windows Server 2003. As a RADIUS server, NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless and virtual private network (VPN) connections. As a RADIUS proxy, NPS forwards authentication and accounting messages to other RADIUS servers. NPS also acts as a health evaluation server for Network Access Protection (NAP).	http://www.microsoft.com/windows/products/windowsvista/enterprise/benefits/operatingsystem.mspx?tab=Improve%20Security%20and%20Compliance
Public Key Infrastructure	Microsoft Public Key Infrastructure (PKI) for Windows Server 2003 provides an integrated public key infrastructure that enables you to secure and exchange information with strong security and easy administration across the Internet, extranets, intranets, and applications.	http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx
Certificates	Windows Certificate Services (CS) provides an integrated public key infrastructure that enables the secure exchange of information. With strong security and easy administration across the Internet, extranets, intranets, and applications, CS provides customizable services for issuing and managing the certificates used in software security systems employing public key technologies.	http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication.mspx
Microsoft Identity Lifecycle Manager	Microsoft Identity Lifecycle Manager 2007 (ILM 2007) provides an integrated and comprehensive solution for managing the entire lifecycle of user identities and their associated credentials. It provides identity synchronization, certificate and password management, and user provisioning in a single solution that works across Microsoft Windows and other organizational systems. As a result, IT organizations can define and automate the processes used to manage identities from creation to retirement.	http://www.microsoft.com/windowsserver2003/technologies/idm/ILM.mspx
Gestión y control		

Subcategoría	Mejores prácticas recomendadas
Informes sobre incidentes y respuesta	Continúe aplicando y siguiendo procedimientos de creación de informes y respuesta ante incidentes formales. Establezca procedimientos para la creación de informes de incidentes y sus respuestas, problemas o preocupaciones sobre seguridad. Designe un equipo de respuesta de emergencia que incluya representantes de varias disciplinas, incluidas tecnología, recursos humanos y legal para responder a todos los incidentes y problemas de seguridad. Considere la posibilidad de implementar un programa completo de respuesta a incidentes que incluya equipos de respuesta a incidentes, gestión de contención, correlación y análisis de eventos, y procedimientos de repuesta a incidentes. Revise este elemento abierto con su personal de TI o un socio de seguridad. Escriba la respuesta más apropiada a esta pregunta en MSAT para obtener más información. Los planes de recuperación ante desastres y de reanudación de negocio deben estar bien documentados y actualizados para asegurar la recuperación en un período de tiempo aceptable. Los planes (incluida la restauración a partir de copias de seguridad para aplicaciones) se deben probar periódicamente para validar el grado de corrección e integridad. Los planes de continuidad de negocio se deben centrar en todo el entorno: físico, tecnológico y personal. Es importante seguir un proceso de creación de informes de incidentes y repuesta documentado para garantizar que todos los problemas e incidentes se revisan y se evalúan de forma coherente. Es importante que todos los usuarios comprendan su responsabilidad de notificar los problemas o incidentes de seguridad y que tengan un proceso definido claramente para notificar estos problemas.

Subcategoría	Mejores prácticas recomendadas	
Creación segura		
	Resultados	**Recomendaciones**
Creación segura	Sus respuestas indican que se han instalado cortafuegos particulares en todas las estaciones de trabajo del entorno.	Al principio, piense en utilizar cortafuegos particulares en cada equipo portátil. De manera predeterminada, bloquee todo acceso a la estación de trabajo desde el exterior.
Creación segura	Sus respuestas indican que los procesos de creación de los dispositivos de infraestructura están documentados.	Implante un proceso de creación documentado para los dispositivos de infraestructura y asegúrese de que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Creación segura	Sus respuestas indican que no hay software de acceso remoto del lado del cliente instalado en las estaciones de trabajo que se conectan remotamente a la red corporativa.	Considere utilizar software de acceso remoto en todas las estaciones individuales, si se necesita conectividad remota. Configure el software de cliente para seguir la directiva de servidores de acceso remoto.
Creación segura	Sus respuestas indican que los procesos de creación de los servidores están documentados.	Implante un proceso de creación documentado para los servidores y asegúrese de que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Creación segura	Sus respuestas indican que no utiliza ningún software de cifrado de discos en el	Piense en utilizar software de cifrado de discos con el fin de no poner en peligro la

	entorno.	confidencialidad de los datos en caso de robo del equipo.
Creación segura	Sus respuestas indican que los procesos de creación de las estaciones de trabajo y los portátiles están documentados.	Implante un proceso de creación documentado para las estaciones de trabajo y los portátiles, y asegúrese de que se mantiene la creación actualizada a medida que se publican nuevas actualizaciones.
Creación segura	Sus respuestas indican que utiliza algún software de control/gestión remota en el entorno.	Considere la deshabilitación del software de gestión/control remoto para reducir el riesgo de intrusiones en los sistemas.
Creación segura	Sus respuestas indican que utiliza un protector de pantalla protegido por contraseña en el entorno.	Continúe con la práctica de exigir a todos los usuarios que tengan un protector de pantalla protegido por contraseña con un tiempo de espera breve.
Creación segura	Sus respuestas indican que no se utilizan módems en el entorno.	Continúe la deshabilitación del acceso por módem y marcación telefónica para reducir el riesgo de que se pueda acceder directamente a los equipos mediante marcación.

Subcategoría	**Mejores prácticas recomendadas**	
Seguridad física	Continúe implementando controles de acceso de seguridad física. Establezca controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considere la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumente la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas. Todos los equipos informáticos se deben proteger contra robos. Los servidores y los equipos de red deben asegurarse en ubicaciones cerradas con acceso controlado. El acceso físico se debe controlar estrictamente, evitando que las personas no autorizadas accedan a edificios, datos confidenciales y sistemas. Con este acceso, pueden alterar las configuraciones del sistema, introducir vulnerabilidades en la red o incluso destruir o robar equipos.	
	Resultados	**Recomendaciones**
Seguridad física	Sus respuestas indican que se han instaurado controles de seguridad física para proteger los activos de la empresa.	Continúe utilizando los controles físicos y considere su uso en todos los equipos informáticos en caso de que aún no se haya realizado.
Seguridad física	Sus respuestas indican que no se ha instalado ningún sistema de alarma para detectar ni informar de intrusiones	Considere la instalación de un sistema de alarma con el fin de detectar e informar de intrusiones.
Seguridad física	La respuesta indica que todo o parte de lo siguiente está implementado. (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada)	Continúe implementando controles de acceso de seguridad física.
Seguridad física	Sus respuestas indican que los equipos de la red se hallan en una habitación cerrada con acceso restringido.	Continúe con la práctica de proteger equipo de red en una habitación cerrada y asegúrese de que únicamente acceden los que deben hacerlo por alguna actividad

		relacionada con la empresa.
Seguridad física	La respuesta indica que (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada) no están implementados.	Establezca controles de acceso físico como protección contra personas no autorizadas que acceden al edificio y a información confidencial. Considere la posibilidad de volver a evaluar todos los controles de acceso físico para garantizar que son adecuados y que se cumplen. Aumente la concienciación del personal sobre las directivas de control de acceso del personal y fomente la duda ante personas desconocidas.
Seguridad física	Sus respuestas indican que los equipos de la red se encuentran además en un armario cerrado.	Si el equipo de red se encuentra en un armario cerrado, la protección contra la manipulación no autorizada es adicional. Asegúrese de que el acceso a las llaves/ combinaciones se limita a aquéllos que únicamente lo necesitan por alguna actividad relacionada con la empresa.
Seguridad física	La respuesta indica que todo o parte de lo siguiente está implementado. (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada)	Continúe implementando controles de acceso de seguridad física.
Seguridad física	Sus respuestas indican que los servidores se hallan en una habitación cerrada con acceso restringido.	Continúe la práctica de asegurar los servidores en una habitación cerrada y asegúrese de que únicamente acceden los que deben hacerlo por alguna actividad relacionada con la empresa.
Seguridad física	La respuesta indica que todo o parte de lo siguiente está implementado. (tarjetas de identificación para empleados y visitantes, acompañantes de visitantes, registros de visitantes, controles de entrada)	Continúe implementando controles de acceso de seguridad física.
Seguridad física	Sus respuestas indican que los servidores se encuentran además en un armario cerrado.	Si los servidores se encuentra en un armario cerrado, la protección contra la manipulación no autorizada es adicional. Asegúrese de que el acceso a las llaves/ combinaciones se limita a aquéllos que únicamente lo necesitan por alguna actividad relacionada con la empresa.
Seguridad física	Sus respuestas indican que las estaciones de trabajo no están protegidas con cables de seguridad.	Para evitar robos, considere asegurar las estaciones de trabajo con cables de seguridad.
Seguridad física	Sus respuestas indican que los ordenadores portátiles no están protegidos con cables de seguridad.	Para evitar robos, considere asegurar los portátiles mediante cables de seguridad.
Seguridad física	Sus respuestas indican que los materiales impresos confidenciales no se almacenan en armarios con llave.	Los documentos confidenciales deberían guardarse en armarios cerrados para que no resulten robados ni se revele información confidencial.

Gestión y control - Recursos		
Windows Server 2008	Windows Server 2008 is the most secure Windows Server yet. The operating system has been hardened to help protect against failure and several new technologies help prevent unauthorized connections to your networks, servers, data, and user accounts. Network Access Protection (NAP) helps ensure that computers that try to connect to your network comply with your organization's security policy. Technology integration and several enhancements make Active Directory services a potent unified and integrated Identity and Access (IDA) solution and Read-Only Domain Controller (RODC) and BitLocker Drive Encryption allow you to more securely deploy your AD database at branch office locations.	http://www.microsoft.com/windowsserver2008/en/us/overview.aspx
Windows Server Active Directory	A central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. Windows Server 2003 makes Active Directory simpler to manage, easing migration and deployment. Windows Server Active Directory is already used by companies around the world to gain unified management of identities and resources across the enterprise network. Active Directory enables organizations to centrally manage and track information about users and their privileges. In addition, Active Directory Lightweight Directory Services (ADLDS), an LDAP directory service, provides organizations with flexible support for directory-enabled applications. Integration with Microsoft Federated Identity, Strong Authentication, Information Protection and Identity Lifecycle Management solutions, makes Active Directory an ideal foundation for building a comprehensive identity and access solution.	http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx http://www.microsoft.com/windowsserver2003/technologies/idm/DirectoryServices.mspx
Public Key Infrastructure	Microsoft Public Key Infrastructure (PKI) for Windows Server 2003 provides an integrated public key infrastructure that enables you to secure and exchange information with strong security and easy administration across the Internet, extranets, intranets, and applications.	http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx
Certificates	Windows Certificate Services (CS) provides an integrated public key infrastructure that enables the secure exchange of	http://www.microsoft.com/windowsserver2003/technologies/idm/StrongAuthentication.mspx

	information. With strong security and easy administration across the Internet, extranets, intranets, and applications, CS provides customizable services for issuing and managing the certificates used in software security systems employing public key technologies.	
Forefront Client Security	Forefront Client Security helps guard against emerging threats, such as spyware and rootkits, as well as traditional threats, such as viruses, worms, and Trojan horses. By delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities, Forefront Client Security helps you protect your business with confidence and efficiency. Forefront Client Security integrates with your existing infrastructure software, such as Microsoft Active Directory, and complements other Microsoft security technologies for enhanced protection and greater control.	http://www.microsoft.com/forefront/clientsecurity/en/us/overview.aspx
Windows Vista - BitLocker Drive Encryption	Bitlocker Drive Encryption is a data protection feature available in Windows Vista Enterprise and Ulitmate editions and in Windows Server 2008. Bitlocker enhances data protection by bringing together drive encription and integrity checking of early boot components.	http://www.microsoft.com/windows/products/windowsvista/features/details/bitlocker.mspx
Windows Vista - Encrypted File System (EFS)	Encrypting File System (EFS) is a data protection feature in the Business, Enterprise and Ultimate editions of Windows Vista. If is userful for user-level file and folder encryption.	http://www.microsoft.com/windows/products/windowsvista/features/details/encryptingfilesystem.mspx
Windows Vista and XPsp2 - Windows Defender	Windows Defender works with Internet Explorer 7 to help make conscious choices installing software on your PS by providing always-on protection and monitoring of key system locations watching for changes that signal the installation and presence of spyware.	http://www.microsoft.com/windows/products/windowsvista/features/details/defender.mspx
Windows Firewall	Windows Firewall is a critiacal first line of defense to protect your computer against many types of malicious software. It can help stop malware before it infects your computer. Windows Firewall comes with Windows Vista and is turned on by default to protect your system as soon as windows starts.	http://www.microsoft.com/windows/products/windowsvista/features/details/firewall.mspx
Windows Security Center	Windows Security Center alers you when your security software is out of date or when your security settings should be strengthened. It displays your firewall settings and tells you whether your PC is set up to receive automatic updates from	http://www.microsoft.com/windows/products/windowsvista/features/details/securitycenter.mspx

	Microsoft.	
Windows Live One Care	Protect, maintain, and manage your computer with Windows Live OneCare, the always-on PC-care service from Microsoft. Working quietly in the background on your computer, OneCare protects against viruses, spyware, hackers, and other unwanted intruders. New features allow for multi-PC management to form a circle of protection, printer sharing support, and centralized backup of up to three PCs covered under the same OneCare subscription.	http://onecare.live.com/standard/en-us/default.htm
ISA Server	Internet Security and Acceleration (ISA) Server 2006 is the integrated edge security gateway that helps protect IT environments from Internet-based threats while providing users with fast and secure remote access to applications and data.Deploy ISA Server 2006 for Secure Remote Access, Branch Office Security, and Internet Access Protection.	http://www.microsoft.com/forefront/edgesecurity/iap.mspx http://www.microsoft.com/forefront/edgesecurity/sra.mspx http://www.microsoft.com/forefront/edgesecurity/bos.mspx
ADFS	Microsoft Active Directory Federation Services (ADFS) provides the interoperability required to simplify the broad, federated sharing of digital identities and policies across organizational boundaries. Seamless yet secure, customers, partners, suppliers, and mobile employees can all securely gain access to the information they need, when they need it. ADFS Boost cross-organizational efficiency and collaboration with secure data access across companies and Improves operational efficiency with streamlined federation systems and simplified management of IDs and passwords. It boost visibility into cross-boundary processes with transparent, auditable information rights and roles and improves security with ADFS claim mapping, SAML tokens, and Kerberos authentication. ADFS helps to reduce operations costs by taking advantage of existing investments in Active Directory and security systems and eliminates the complexity of managing federation by using Active Directory as the main identity repository.	http://www.microsoft.com/windowsserver2003/technologies/idm/federatedidentity.mspx
(IPV6) Direct Connect	IPv6 is designed to solve many of the problems of the current version of IP (known as IPv4) such as address depletion, security, autoconfiguration, and extensibility. Its use will also expand the capabilities of the Internet to enable a variety of valuable and exciting scenarios,	http://technet.microsoft.com/en-us/network/bb530961.aspx

	including peer-to-peer and mobile applications. Support for Internet Protocol version 6 (IPv6), a new suite of standard protocols for the Network layer of the Internet, is built into the latest versions of Microsoft Windows, which include Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP with Service Pack 2, Windows XP with Service Pack 1, Windows XP Embedded SP1, and Windows CE .NET.	
IPSec	Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group. IPsec is supported by the Microsoft Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP, and Windows 2000 operating systems and is integrated with the Active Directory directory service. IPsec policies can be assigned through Group Policy, which allows IPsec settings to be configured at the domain, site, or organizational unit level.	http://technet.microsoft.com/en-us/network/bb531150.aspx
802.1	The IEEE 802.1X standard for wired networks provides authentication and authorization protection at the network edge where a host attaches to the network. IPsec provides peer authentication and cryptographic protection of IP traffic from end-to-end. This white paper describes the security and capabilities of 802.1X for wired networks and IPsec based on industry standards and their support in Windows Server 2003, Windows Server 2008, Windows XP and Windows Vista and provides comparison information when evaluating deployment of these security technologies.	http://technet2.microsoft.com/windowsserver/en/library/908d13e8-c4aa-4d62-8401-86d7da0eab481033.mspx?mfr=true

Aplicaciones

Una comprensión total de la seguridad de las aplicaciones requiere un conocimiento profundo de la arquitectura de las aplicaciones subyacentes básicas, así como de un conocimiento sólido de la base de la aplicación del usuario. Sólo entonces podrá comenzar a

identificar las posibles amenazas.

Teniendo en cuenta el ámbito limitado de esta autoevaluación, no es posible un análisis completo de la arquitectura de las aplicaciones ni una comprensión completa de la base del usuario. El objetivo de esta evaluación consiste en ayudarle a revisar las aplicaciones de su empresa y valorarlas desde el punto de vista de la seguridad y disponibilidad. Examina las tecnologías utilizadas en el entorno para contribuir a mejorar la defensa en profundidad. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar los riesgos para la infraestructura centrándose en las siguientes áreas de seguridad:

- Utilización y uso—mecanismos para mejorar la disponibilidad
- Diseño de aplicaciones —autenticación, control de acceso, gestión de actualizaciones, validación de datos de entrada, registros y auditorías
- Almacenamiento y comunicaciones de datos—cifrado,transferencia de datos, acceso restrictivo

Implementación y uso		
Subcategoría	**Mejores prácticas recomendadas**	
Equilibrio de carga		
	Resultados	**Recomendaciones**
Equilibrio de carga	Sus respuestas indican que no se utilizan equilibradores de carga en el entorno.	Piense en utilizar equilibradores de carga de hardware en el primer nivel de los servidores Web para obtener una mayor disponibilidad. El equilibrador de carga muestra una sola dirección IP (virtual) al exterior que se asigna a todas las direcciones de cada servidor Web en el clúster.
Subcategoría	**Mejores prácticas recomendadas**	
Clústeres		
	Resultados	**Recomendaciones**
Clústeres	Sus respuestas indican que no se utiliza la agrupación en clústeres en el entorno.	Para asegurar una disponibilidad alta de las bases de datos críticas y de los archivos compartidos, piense en utilizar mecanismos de clúster.
Subcategoría	**Mejores prácticas recomendadas**	
Aplicación y recuperación de datos		
	Resultados	**Recomendaciones**
Aplicación y recuperación de datos	Sus respuestas indican que su empresa no tiene ninguna línea de aplicaciones empresariales	Al no tener ninguna aplicación de línea comercial de propósito crítico, se evita el riesgo de que tales sistemas fallen. Sin embargo, si prevé utilizar alguna en el futuro, estas aplicaciones deberían evaluarse periódicamente para su seguridad, someterse a procesos regulares

		de copias de seguridad, documentarse a fondo y contar con planes de contingencia en caso de que se produzcan fallos.
Aplicación y recuperación de datos	Su respuesta indica que no se realizan periódicamente pruebas de la recuperación de aplicaciones y datos.	Realice copias de seguridad regularmente. Pruebe regularmente el mecanismo de copias de seguridad y recuperación que restaura la aplicación a un estado normal de operación.

Subcategoría	**Mejores prácticas recomendadas**
Fabricante de software independiente (ISV)	Los fabricantes de software independiente (ISV) deben ofrecer revisiones y actualizaciones periódicas, en las que se explique su finalidad y las consecuencias derivadas de su uso en términos de funcionalidad, configuración y seguridad. El ISV debe identificar claramente cuáles son las actualizaciones más importantes para que se apliquen rápidamente. Asimismo, debe describir los distintos mecanismos de seguridad de la aplicación y proporcionar la documentación más reciente. La empresa debe conocer las configuraciones necesarias para garantizar el nivel de seguridad más alto.

	Resultados	**Recomendaciones**
Fabricante de software independiente (ISV)	Sus respuestas indican que otros fabricantes han desarrollado una o más de las aplicaciones principales del entorno.	Asegúrese de que podrá seguir disponiendo de servicio técnico y actualizaciones periódicas para los software clave de su empresa, o que el fabricante independiente de los mismos puede ofrecerle el código de origen en caso de que ya no pueda prestar dicho servicio para la aplicación.
Fabricante de software independiente (ISV)	Su respuesta indica que los fabricantes independientes de software no le suelen ofrecer revisiones ni actualizaciones de seguridad.	Intente colaborar con el fabricante de aplicaciones para recibir actualizaciones y revisiones lo más frecuentemente posible. Cuando aparezca una actualización, pruébela completamente en el entorno de laboratorio antes de utilizarla. Intente conseguir la documentación para reforzar la aplicación del ISV, si existe, y revise las configuraciones de la aplicación.
Fabricante de software independiente (ISV)	Sus respuestas indican que no conoce la respuesta a esta pregunta	Revise esta opción abierta con su personal de TI o con un socio de seguridad. Introduzca la respuesta más adecuada a esta pregunta en MSAT para obtener más información.

Subcategoría	**Mejores prácticas recomendadas**
Desarrollado internamente	El equipo de desarrollo interno debe proporcionar las actualizaciones y revisiones e indicar cuál es la finalidad de la actualización y las consecuencias derivadas de su uso en términos de funcionalidad, configuración y seguridad. El equipo de desarrollo interno debe identificar claramente cuáles son las

	actualizaciones más importantes para que la empresa pueda instalarlas rápidamente. El equipo de desarrollo debe describir los distintos mecanismos de seguridad de la aplicación y proporcionar la documentación más actualizada. La empresa debe conocer las configuraciones necesarias para garantizar el nivel de seguridad más alto. Considere la posibilidad de contratar servicios independientes para revisar la arquitectura y utilización de la aplicación y para identificar los problemas de seguridad que pudieran existir.	
	Resultados	**Recomendaciones**
Desarrollado internamente	Sus respuestas indican que su empresa no utiliza macros personalizadas en las aplicaciones ofimáticas.	No continúe utilizando macros de Office personalizadas, ya que es necesario que las configuraciones de seguridad de Office se reclasifiquen a un nivel inferior, por lo que sus aplicaciones ofimáticas quedan expuestas a documentos peligrosos.
Desarrollado internamente	Su respuesta indica que su equipo interno de desarrollo de software no le suele ofrecer revisiones ni actualizaciones de seguridad.	Intente trabajar con el equipo de desarrollo interno para recibir periódicamente revisiones y actualizaciones de las aplicaciones utilizadas. Cuando aparezca una revisión, pruébela completamente en el entorno de laboratorio antes de utilizarla. Trabaje con el equipo de desarrollo para revisar las configuraciones de las aplicaciones y garantizar así una máxima seguridad. Piense en contratar a un tercero para revisar la arquitectura y utilización de la aplicación y para detectar posibles problemas de seguridad.
Subcategoría	**Mejores prácticas recomendadas**	
Vulnerabilidades	Debe identificar y corregir todas las vulnerabilidades de seguridad conocidas. Visite los sitios de los fabricantes y otros proveedores de soluciones de seguridad para buscar información sobre nuevas vulnerabilidades, así como las actualizaciones disponibles. Si no existen actualizaciones disponibles para vulnerabilidades de seguridad conocidas, intente averiguar cuándo podrá disponer de una y desarrolle un plan de seguridad provisional. Puede contratar servicios independientes para revisar regularmente el diseño de seguridad de la aplicación. Una evaluación realizada por terceros podría descubrir otros problemas que exijan mecanismos de seguridad adicionales.	
	Resultados	**Recomendaciones**
Vulnerabilidades	Su respuesta indica que actualmente no se conocen vulnerabilidades para la seguridad en ninguna aplicación de su	Visite los sitios de los fabricantes y otros proveedores de soluciones de seguridad para detectar vulnerabilidades de la

	entorno.	aplicación. Piense en una evaluación independiente para que un tercero pueda valorar el diseño de la seguridad de la aplicación e identificar otros problemas que necesiten más mecanismos de seguridad.

Implementación y uso - Recursos		
2007 Office Security Guide	As risks from malicious attack have increased, desktop application security mechanisms have evolved. The new security model in the 2007 Microsoft Office release provides new mechanisms, settings, and features that allow your organization to achieve an effective balance between protection and productivity while minimizing user disruption. You might think that such risks come from outside your organization, and can therefore be stopped by effective network security mechanisms such as firewalls, proxy servers, and intrusion detection systems. However, many of these business risks can come from internal users and unsecured systems that are at the heart of your organization. Unless securely configured, the desktop applications that your information workers rely on to send e-mail, write documents, create presentations, and analyze data can be critical pathways for attack by malicious software (malware), including spyware, Trojan horses, viruses, and worms.	http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/default.mspx
Microsoft Rights Management Services for Windows Server 2003	Microsoft Windows Rights Management Services (RMS) for Windows Server 2003 is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use—both online and offline, inside and outside of the firewall. RMS augments an organization's security strategy by protecting information through persistent usage policies, which remain with the information, no matter where it goes. Organizations can use RMS to help prevent sensitive information—such as financial reports, product specifications, customer data, and confidential e-mail messages—from intentionally or accidentally getting into the wrong hands. This services is built into Windows Server 2008 as Active Directory Rights	http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx

	Management Services (ADRMS)	
Windows Server 2008 - Active Directory Rights Management Services	Windows Server 2008 - Active Directory Rights Management Services (AD RMS) is an information protection technology that works with AD RMS-enabled applications (Office 2007) to help safegaurd digital information from unauthorized use. Content owners can define who can open, modify, print, forward or take other actions with the information.	http://technet2.microsoft.com/windowsserver2008/en/library/37c240d3-8928-4267-867b-4c005b72cca21033.mspx?mfr=true
Windows Server 2008 - Clustering	Failover clustering in Windows Server 2008 can help you build redundancy into your network and eliminate single points of failure. The improvements to failover clusters (formerly known as server clusters) in Windows Server 2008 are aimed at simplifying clusters, making them more secure, and enhancing cluster stability. All of which helps reduce downtime, guard against data loss, and reduce your total cost of ownership. Because they are included in the enhanced-capability editions of Windows Server 2008, such as Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, Windows Server 2008 failover clusters are much less expensive than comparable systems, which can cost thousands of dollars. Ease of deployment and affordability make Windows Server 2008 an ideal high-availability solution for organizations of all sizes.	http://www.microsoft.com/windowsserver2008/en/us/clustering-home.aspx
Microsoft Security Development Lifecycle	Trustworthy Computing is a Microsoft initiative for ensuring the production of secure code. A key element of the Trustworthy Computing initiative is the Microsoft Security Development Lifecycle (SDL). The SDL is an engineering practice that is used in conjunction with standard engineering processes to facilitate the delivery of secure code. The SDL consists of ten phases that combine best practices with formalization, measurability, and additional structure, including: security design analysis, tool-based quality checks, penetration testing, final security review, post release product security management. This methodology is also available in book form through Microsoft Press.	http://msdn.microsoft.com/en-us/library/aa969774.aspx

Diseño de aplicaciones	
Subcategoría	**Mejores prácticas recomendadas**

Autenticación	La aplicación debe utilizar un mecanismo de autenticación cuya eficacia sea proporcional a las necesidades de seguridad de los datos o de su funcionalidad. Las aplicaciones que dependen de contraseñas deben requerir contraseñas complejas que incluyan diversos caracteres (alfabéticos, numéricos, y símbolos), una longitud mínima, un historial, un límite de duración, una pre-caducidad y una comprobación en el diccionario. La aplicación debe archivar los intentos de registro fallidos, pero no la contraseña. Cada componente que concede acceso a datos o a funciones debe requerir una autenticación correcta. Debe proteger el acceso administrativo a los sistemas con los tipos de autenticación más sólidos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las de las cuentas normales. Además de usar contraseñas sólidas con directivas de contraseñas, considere la autenticación multifactor para una mayor seguridad.

Subcategoría	Mejores prácticas recomendadas
Directivas de contraseñas	La utilización de contraseñas sólidas es un elemento fundamental del índice de la defensa en profundidad. Estas contraseñas deben tener entre 8 y 14 caracteres e incluir caracteres alfanuméricos y especiales. Debe establecer una longitud mínima, un historial, un límite a la duración y una caducidad para reforzar la defensa. Generalmente, la caducidad de las contraseñas debe configurarse de esta forma: + Duración máxima de 90 días + Las cuentas nuevas deben cambiar la contraseña al inicio de la sesión + Un historial de 8 contraseñas (mínimo de 8 días) Debe proteger el acceso administrativo a los sistemas con los tipos de autenticación más sólidos. Por lo general, las limitaciones para crear contraseñas de administradores deben ser más estrictas que las que se emplean para cuentas normales: si las cuentas normales requieren contraseñas con 8 caracteres, las cuentas administrativas deben requerir contraseñas de 14 caracteres. Active una práctica de bloqueo de la cuenta tras 10 intentos fallidos en todas las cuentas de usuario. Los controles para bloquear una cuenta pueden variar, algunos simplemente consisten en bloquear ataques de fuerza bruta a contraseñas y otros requieren que un administrador desbloquee la cuenta. Cuando se pongan en práctica controles de bloqueo de cuenta, siga las normas siguientes: + Bloqueo después de 10 intentos de registro fallidos para las cuentas de usuario + Requerir la intervención de un administrador para desbloquear las cuentas de aplicaciones importantes y reactivar automáticamente las cuentas de usuarios normales al cabo de 5 minutos + 30 minutos para almacenar en caché los fallos de cuentas de usuarios normales

	Resultados	Recomendaciones
Directivas de contraseñas	Su respuesta indica que no se usan controles de contraseñas en las aplicaciones principales.	Es importante poner en práctica una directiva de controles de contraseña. Todas las aplicaciones externas e internas importantes con datos confidenciales deben tener directivas de contraseñas. Piense en poner en práctica una directiva que requiera contraseñas complejas, períodos de caducidad de contraseñas y

	umbrales para bloquear las cuentas.

Subcategoría	Mejores prácticas recomendadas
Autorización y control de acceso	Las aplicaciones deben utilizar un mecanismo de autorización que permita sólo a los usuarios o clientes adecuados el acceso a datos y funciones confidenciales. Debe mantener controles de acceso basados en roles, tanto para la base de datos como para la interfaz de la aplicación. De esta forma, se protege la base de datos incluso si la aplicación cliente resulta atacada. Para comprobar una autorización, deberá haberse realizado antes una autenticación con éxito. Se deben archivar todos los intentos de acceso sin autorización adecuada. Compruebe regularmente las aplicaciones principales que procesan datos confidenciales y las interfaces disponibles a los usuarios de Internet. Incluya pruebas de "caja negra" e "informadas" de la aplicación. Descubra si los usuarios pueden acceder a los datos mediante otras cuentas.

	Resultados	Recomendaciones
Autorización y control de acceso	Su respuesta indica que las aplicaciones principales limitan el acceso a datos y funciones confidenciales según los privilegios de la cuenta.	Piense en probar exclusivamente las aplicaciones principales que procesen datos confidenciales y las interfaces disponibles para los usuarios por Internet. Incluya pruebas tipo "caja negra" e "informadas" de la aplicación y compruebe la asignación de mayores privilegios.

Subcategoría	Mejores prácticas recomendadas
Registro	Debe activar archivos de registro en todas las aplicaciones del entorno. Los datos de archivos de registro son importantes para los análisis de incidentes, tendencias y auditorías. La aplicación debe registrar los intentos de autenticación que tienen éxito y los fallidos, además de los cambios de datos de la aplicación, incluidas las cuentas de usuarios, los errores graves de la aplicación y los accesos correctos y fallidos a los recursos. Cuando escriba datos en los archivos de registro, la aplicación deberá evitar los de carácter confidencial.

	Resultados	Recomendaciones
Registro	Sus respuestas indican que hay varios eventos registrados por las aplicaciones del entorno. Las aplicaciones deben registrar todos los eventos según las prácticas recomendadas.	Para facilitar la gestión y el análisis de los archivos de registro, puede integrarlos en un mecanismo de registro central. Este mecanismo guarda estos archivos según la directiva corporativa de retención de datos.
Registro	Sus respuestas indican que se registran los intentos fallidos de autenticación.	Continúe realizando registros de intentos de autenticación fallidos.

Registro	Sus respuestas indican que se registran los intentos de autenticación correctos.	Continúe realizando registros de autenticaciones correctos.
Registro	Sus respuestas indican que se registran los errores de las aplicaciones.	Continúe realizando registros de errores de la aplicación.
Registro	Sus respuestas indican que se registran los accesos denegados a los recursos.	Continúe realizando registros del acceso denegado a los recursos
Registro	Sus respuestas indican que se registran los accesos correctos a los recursos.	Continúe realizando registros del acceso correcto a los recursos
Registro	Sus respuestas indican que no se registran los cambios en los datos.	Considere realizar registros de las modificaciones de los datos para realizar un seguimiento de las actividades contraproducentes.
Registro	Sus respuestas indican que no se registran los cambios en las cuentas de usuario.	Considere realizar registros de las modificaciones de las cuentas de usuarios para detectar asignaciones de mayores privilegios y creaciones de cuentas nuevas no autorizadas.

Subcategoría	**Mejores prácticas recomendadas**
Validación de datos de entrada	La aplicación puede permitir la entrada de datos en distintos puntos a partir de fuentes externas, como, por ejemplo, usuarios, aplicaciones de cliente o bien alimentación de datos. Será necesario comprobar que los datos de entrada tengan una sintaxis y semántica correctas. Por otro lado, se comprobará si tales datos cumplen las restricciones de los componentes subyacentes o dependientes, particularmente la longitud de cadenas y los juegos de caracteres. El servidor deberá validar los campos suministrados por el usuario.

	Resultados	**Recomendaciones**
Validación de datos de entrada	Sus respuestas indican que no se utilizan mecanismos para validar los datos de entrada en las aplicaciones del entorno.	Colabore con el fabricante de la aplicación (fabricante independiente de software o equipo de desarrollo interno) para implantar mecanismos de validación de los datos de entrada, para que la aplicación no procese datos peligrosos ni incorrectos. Al principio, estos módulos deben ponerse en práctica para las aplicaciones externas. Las restricciones de validación de datos de entrada deben permitir datos con sintaxis y semántica correctas y no efectuar únicamente el análisis para la detección de caracteres no válidos.

Subcategoría	**Mejores prácticas recomendadas**
Metodologías de desarrollo de seguridad de software	Continúe utilizando las metodologías de desarrollo de seguridad de software. Establezca el uso de metodologías de desarrollo de seguridad de software para aumentar la seguridad de las aplicaciones. Si se utilizan consultores o proveedores en alguna fase del ciclo de desarrollo, asegúrese de que tienen formación en la metodología de desarrollo de seguridad de software que la organización utilice o recomiende. Todo el personal de desarrollo de su organización debe recibir formación sobre la

	metodología de desarrollo de seguridad para software que la organización ha elegido. Esto incluye administradores de desarrollo, desarrolladores, evaluadores y personal de control de calidad. Con el panorama de evolución de amenazas de seguridad, es importante actualizar la formación sobre metodologías de desarrollo de seguridad de software y modelos de amenazas anualmente. Se le solicitará al personal de desarrollo que siga la formación sobre desarrollo de seguridad cada año. El uso de herramientas de prueba de software de seguridad mejora la capacidad del equipo para escribir código seguro con más eficacia. El resultado del uso de las herramientas de prueba se debe incorporar a la formación anual necesaria.

	Resultados	**Recomendaciones**
Metodologías de desarrollo de seguridad de software	La respuesta indica que su organización no proporciona formación sobre metodologías de seguridad para software para su personal de desarrollo.	Establezca un programa de formación de metodologías de desarrollo de seguridad de software con el objeto de mejorar la capacidad del personal para desarrollar código seguro.
Metodologías de desarrollo de seguridad de software	La respuesta indica que su organización no utiliza herramientas de pruebas de software de seguridad como parte del proceso de desarrollo de seguridad.	Establezca el uso de las herramientas de prueba de software de seguridad como parte instrumental de todos los planes de desarrollo de seguridad.

Almacenamiento y comunicaciones de datos	
Subcategoría	**Mejores prácticas recomendadas**
Cifrado	Los datos confidenciales deben cifrarse o codificarse mediante hash en la base de datos y en el sistema de archivos. La aplicación debe diferenciar entre los datos que podrían estar expuestos a la divulgación (es necesario cifrarlos), los datos que podrían llegar a manipularse (es necesario un valor de claves hash) y los datos que se pueden transformar (hash) sin ninguna pérdida de funcionalidad, como las contraseñas. Las claves para descifrar se guardarán en un lugar distinto a la información cifrada. Los datos confidenciales se deben cifrar antes de transmitirlos a otros componentes. Verifique que los componentes intermedios que controlan los datos en un formato de texto sin formato antes o después de la transmisión no representan una amenaza excesiva. La aplicación debe sacar partido de las funciones de autenticación disponibles con el mecanismo de transmisión segura. Algunos de los cifrados más habituales y fiables son: 3DES, AES, RSA, RC4 y Blowfish. Utilice claves de 128 bits (1024 bits para RSA) como mínimo.

	Resultados	**Recomendaciones**
Cifrado	Sus respuestas indican que sus aplicaciones no cifran los datos cuando están almacenados o se están transmitiendo.	Para aplicaciones que procesan datos confidenciales, opte por el cifrado con un algoritmo estándar del sector para la transmisión y el almacenamiento de datos.

Subcategoría	**Mejores prácticas recomendadas**
Cifrado - Algoritmo	La aplicación debe utilizar algoritmos de cifrado estándares del sector, con claves de tamaños adecuados y modelos de cifrado apropiados. Algunos de los cifrados más habituales y fiables son: 3DES, AES, RSA, RC4 y Blowfish. Se debe utilizar un tamaño de clave mínimo de 128 bits (para RSA, 1024 bits).

Operaciones

Los esfuerzos de seguridad en una empresa a menudo pasan por alto los aspectos que son críticos para la ayuda del mantenimiento de la seguridad general en la empresa. Esta sección de la evaluación revisa aquellos procesos de la empresa que regulan las directivas de seguridad corporativas, los procesos de recursos humanos, así como la formación y la divulgación de materias de seguridad para los empleados. El área de análisis de personal también se centra en la seguridad, ya que relaciona las tareas diarias operativas y las definiciones de los roles. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar los riesgos del personal centrándose en las siguientes áreas de la seguridad del personal:

- Requisitos y evaluaciones—planificación, evaluaciones de terceros
- Directiva y procedimientos—directiva de RR.HH., relaciones con terceros
- Formación y conocimiento—divulgación de las medidas de seguridad

Requisitos y evaluaciones		
Subcategoría	**Mejores prácticas recomendadas**	
Requisitos de seguridad	La empresa identifica a los individuos con experiencia en el tema de la seguridad para incluirlos en todas las reuniones y decisiones relacionadas. Además, señala qué debe protegerse, teniendo en cuenta el valor del recurso y el nivel de seguridad que se requiere. El análisis incluye todas las amenazas posibles. La estrategia que resulta equilibra los costes y los beneficios de las protecciones, y puede incluir como opciones el traslado o la aceptación de los riesgos. Los requisitos de seguridad, definidos por representantes comerciales y técnicos, se documentan y publican para que el conjunto del personal los pueda consultar y contrastar para diseños futuros. Las diferencias entre los tipos de aplicaciones y de datos pueden dar como resultado la existencia de requisitos diferentes.	
	Resultados	**Recomendaciones**
Requisitos de seguridad	Sus respuestas indican que su empresa tiene un modelo para la asignación de niveles de gravedad a cada componente del entorno informático.	Continúe asignando niveles de importancia a los componentes y asegúrese de actualizar el modelo según se añada al equipo nuevo.
Requisitos de seguridad	Su respuesta indica que existen equipos comerciales y de seguridad que trabajan definiendo requisitos de seguridad.	El equipo de seguridad debe tomar parte en todos los aspectos de los requisitos, diseño y utilización de tecnologías. Se deben documentar requisitos claros para las especificaciones de funcionamiento.
Subcategoría	**Mejores prácticas recomendadas**	
Evaluaciones de seguridad	Las evaluaciones por parte de terceros aportan una perspectiva objetiva muy valiosa para las medidas de seguridad de una empresa. Estas evaluaciones también podrían resultar beneficiosas para cumplir las estipulaciones normativas y los requisitos de los clientes, socios y fabricantes. Las evaluaciones deben incluir la infraestructura, las aplicaciones, las directivas y los procedimientos de auditoría. Estas evaluaciones no deben centrarse exclusivamente en la identificación de vulnerabilidades, sino también en señalar configuraciones que no sean seguras o privilegios de acceso innecesarios. Se deben revisar las directivas y los procedimientos de seguridad para descubrir si tienen lagunas.	

	Resultados	Recomendaciones
Evaluaciones de seguridad	Su respuesta indica que no encarga a empresas independientes la evaluación de los medios de seguridad.	Empiece con autoevaluaciones de la infraestructura crítica de red y de las aplicaciones. Estudie desarrollar un plan que solicite evaluaciones regulares realizadas por terceros para la infraestructura crítica de red y de las aplicaciones. Incluya los resultados de las evaluaciones en sus proyectos de mejora.
Evaluaciones de seguridad	Sus respuestas indican que las evaluaciones de la seguridad de su empresa no las realiza personal interno.	Piense en el personal interno para la realización de auditorías de seguridad frecuentes, pero debe aumentar estas auditorías con los datos de un tercero de confianza.

Directiva y procedimientos	
Subcategoría	**Mejores prácticas recomendadas**
Comprobaciones del historial personal	Se deben realizar comprobaciones del historial personal para descubrir cualquier problema posible, con objeto de reducir el riesgo al que se exponen la empresa y los empleados. Este proceso también permite localizar cualquier problema o laguna en el currículum del aspirante. El proceso de contratación de personal debe incluir una evaluación del historial laboral y cualquier antecedente penal del aspirante. Se deben evaluar las habilidades del aspirante comparándolas con las descripciones detalladas y los requisitos del puesto para detectar los puntos fuertes y débiles.

	Resultados	Recomendaciones
Comprobaciones del historial personal	Su respuesta indica que se hacen comprobaciones del historial personal de todos los empleados.	Excelente, siga con esta directiva. Asegúrese de que la comprobación del historial personal incluye una evaluación del historial laboral, la formación y los antecedentes penales del aspirante.

Subcategoría	**Mejores prácticas recomendadas**
Directiva de recursos humanos	Los procedimientos formales para gestionar el caso de los empleados que dejan la empresa garantizan que se actúa debidamente cuando se rescinde un contrato de trabajo. Estos procedimientos deben existir para gestionar la situación de los empleados que dejan la empresa amistosamente y los que la dejan de forma hostil. Estos procedimientos deben incluir: + Notificación a todos los departamentos (Recursos humanos, TI, Seguridad física, Servicio de atención al cliente, Finanzas, etc.) + Acompañamiento del empleado al abandonar las instalaciones + Cancelación de todas las cuentas del usuario y de su acceso a la red + Recuperación de todos los bienes de la empresa (portátiles, PDA, dispositivos electrónicos, documentos confidenciales, etc.)

	Resultados	Recomendaciones
Directiva de recursos humanos	Su respuesta indica que no existe ninguna directiva formal para los empleados que dejan la empresa.	Colabore con el departamento de recursos humanos para desarrollar de inmediato una directiva formal para los empleados que dejan la empresa. Contemple los supuestos de ceses amistosos y hostiles del puesto de trabajo. El aspecto más importante que se debe recoger en esta directiva es garantizar que ninguno de los empleados pueden acceder físicamente a los recursos ni a los privilegios de TI una vez fuera de la empresa.

Subcategoría	Mejores prácticas recomendadas
Relaciones con terceros	Con objeto de reducir el riesgo de revelación de datos, deben existir directivas y procedimientos formales enfocados a las relaciones con terceros. Así, se podrá detectar cualquier problema de seguridad y la responsabilidad de cada parte a la hora de solucionarlo. Estas directivas deben incluir: + El nivel de conectividad y acceso + La presentación y el tratamiento de los datos + Los roles y las responsabilidades (incluida la autoridad) de cada parte + La gestión de la relación: creación, mantenimiento y cese.

	Resultados	Recomendaciones
Relaciones con terceros	Sus respuestas indican que los sistemas se configuran por parte de personal interno.	El personal interno debería configurar los sistemas siguiendo una simulación de creación.
Relaciones con terceros	Sus respuestas indican que su empresa gestiona el entorno informático.	Según las necesidades de la empresa, pueden ser soluciones viables tanto la gestión propia como la subcontratada. Si se subcontratan los servicios, los requisitos de seguridad deberían tratarse en el contrato y los acuerdos de nivel de servicio (SLA) deberían garantizar el cumplimiento de tales requisitos.
Relaciones con terceros	Su respuesta indica que no existe ninguna directiva para las relaciones con terceros.	Debe desarrollar directivas y procedimientos formales para los distintos tipos de relaciones con terceros con el acuerdo común de toda la empresa. Para ello, haga partícipe a los diversos equipos empresariales. Si las directivas se elaboran correctamente, los riesgos a los que está expuesta la empresa se verán reducidos.

Formación y conocimiento	
Subcategoría	**Mejores prácticas recomendadas**
Conocimiento de seguridad	Un programa formal de divulgación de las medidas de seguridad ayuda a los

	empleados a contribuir a la seguridad global de la empresa, puesto que se les mantiene informados acerca de los riesgos existentes. La mejor garantía de alerta ante problemas potenciales es formar debidamente al personal en materia de seguridad. Un programa de divulgación efectivo debe tener en cuenta todos los aspectos de la seguridad (aplicaciones, redes y soportes físicos) y ofrecer también pautas claras a los empleados en caso de que detecten un riesgo para la seguridad de cualquiera de estos elementos. Ponga en práctica directivas para regular la utilización de los recursos corporativos por parte de los empleados. Los programas de divulgación deben formar parte del curso de orientación de empleados nuevos. Se debe proporcionar información actualizada y cursos para asegurar que todos los empleados conozcan las prácticas y los riesgos más recientes. Se deben realizar comprobaciones periódicas para asegurarse de que los empleados han asimilado la información.	
	Resultados	**Recomendaciones**
Conocimiento de seguridad	Sus respuestas indican que ha asignado a un individuo o grupo la seguridad de su empresa.	Continúe asegurándose de que su empresa tenga una persona o equipo responsable de la seguridad y requiera que se consulte a este equipo antes de realizar cambios en el entorno informático.
Conocimiento de seguridad	Sus respuestas indican que su equipo de seguridad participa en la definición de los requisitos para las nuevas tecnologías o para las ya existentes.	Continúe realizando consultas al equipo de seguridad antes de realizar cambios en el entorno informático. El equipo de seguridad debería participar en todos las reuniones, desde las primeras fases de planificación.
Conocimiento de seguridad	Su respuesta indica que no existe ningún programa de divulgación de las medidas de seguridad en la empresa.	Evalúe poner en práctica un programa formal de divulgación de seguridad para que los empleados conozcan los riesgos relacionados con los recursos de TI. Ponga en práctica directivas que regulen la utilización de los recursos y las tecnologías corporativas por parte de los empleados e incluya un programa de divulgación de seguridad en el curso de orientación para nuevos empleados. La mejor garantía de alerta ante problemas potenciales es formar debidamente al personal en materia de seguridad.
Subcategoría	**Mejores prácticas recomendadas**	
Formación sobre seguridad	Trabaje con propietarios de empresa para determinar el tiempo de inactividad de aplicaciones críticas. Basándose en esos resultados, aplique las medidas oportunas para satisfacer e incluso superar esos requisitos. La disponibilidad y el rendimiento de las aplicaciones basadas en web mejoran al implementar equilibrio de carga delante de los servidores web. Para equilibrar la carga del servidor, el equilibrio de carga distribuye las solicitudes entre los distintos nodos en el clúster del servidor con el objetivo de optimizar el rendimiento del sistema. Si se produce un error en un servidor web en el	

	clúster del servidor, la solicitud se dirige a otro servidor para atender la solicitud, lo que proporciona una alta disponibilidad. Determine el tiempo de inactividad aceptable para los usos compartidos de archivos y bases de datos de propietarios de empresa. Pruebe los mecanismos de conmutación por error para las aplicaciones y determine si la cantidad del tiempo de inactividad es aceptable.	
	Resultados	**Recomendaciones**
Formación sobre seguridad	Su respuesta indica que la empresa no ofrece actualmente a los empleados formación específica por temas.	En principio y según las exigencias de su modelo empresarial, desarrolle un plan para que el equipo de TI y de desarrollo tenga la formación de seguridad apropiada. Dé comienzo al plan garantizando la asistencia de este equipo a sesiones de formación como seminarios y foros específicos. Redacte el plan para que incluya cualquier tipo de curso básico para todos los empleados en el futuro.

Formación y conocimiento - Recursos		
Microsoft Security Certifications	The MCSE: Security for Windows Server2003 certification provides you the skill set to secure a Windows Server environment.	http://www.microsoft.com/learning/mcp/mcse/security/windowsserver2003.mspx
Industry Security Certifications	(ISC)2 - CISSP, SSCP Certifications ISACA - CISM, CISA Certifications CompTIA - Security+	http://www.isc2.org http://www.isaca.org http://www.comptia.org
Microsoft Security Awareness Toolkit	Microsoft recognizes that information security awareness and training is critical to any organization's information security strategy and supporting security operations. People are in many cases the last line of defense against threats such as malicious code, disgruntled employees, and malicious third parties. Therefore, people need to be educated on what your organization considers appropriate security-conscious behavior, and also what security best practices they need to incorporate in their daily business activities. This kit was created to provide guidance, samples, and templates for creating your own security awareness program.	http://technet.microsoft.com/en-us/security/cc165442.aspx

Lista de acciones recomendadas

La siguiente lista da prioridad a las recomendaciones presentadas anteriormente en la sección Detalles de la evaluación. Para obtener más información sobre cualquiera de estos elementos, consulte la entrada correspondiente en dicha sección.

Un socio de seguridad de Microsoft puede ayudarle a crear un programa de seguridad que se ajuste a estas acciones.

Lista de acciones recomendadas	
Tema del análisis	**Recomendación**
Prioridad alta	
Infraestructura > Autenticación > Usuarios de acceso remoto	Si aún no lo ha hecho, estudie la utilización de un sistema de autenticación multifactor de acceso remoto y limite el acceso únicamente a aquellos empleados que tengan una necesidad empresarial de conectividad remota.
Infraestructura > Defensa del perímetro > Acceso remoto	Utilice VPN para la conectividad de acceso de usuario remoto basada en las tecnologías IPSec, SSL, y SSH. Utilice conectividad sitio-a-sitio basada en la tecnología IPSec. Configure listas de acceso a redes y de usuario para limitar el acceso a los recursos corporativos necesarios.
Infraestructura > Defensa del perímetro > Segmentación	Si los servicios de Internet se exponen a otros servicios que van a albergarse en la red de la empresa, asegúrese de que los cortafuegos, la segmentación y los sistemas de detección de intrusiones protegen la infraestructura de la empresa de los ataques desde Internet.
Infraestructura > Gestión y control > Creación segura	Considere la deshabilitación del software de gestión/control remoto para reducir el riesgo de intrusiones en los sistemas.
Personal > Directiva y procedimientos > Relaciones con terceros	El personal interno debería configurar los sistemas siguiendo una simulación de creación.
Prioridad intermedia	
Infraestructura > Gestión y control > Seguridad física	Continúe utilizando los controles físicos y considere su uso en todos los equipos informáticos en caso de que aún no se haya realizado.
Infraestructura > Defensa del perímetro > Inalámbrico	Para reducir los riesgos asociados a las redes inalámbricas, la implantación no debe incluir la difusión del SSID, pero sí el cifrado WPA, además de tratar la red como de no confianza.
Personal > Formación y conocimiento > Conocimiento de seguridad	Continúe asegurándose de que su empresa tenga una persona o equipo responsable de la seguridad y requiera que se consulte a este equipo antes de realizar cambios en el entorno informático.
Infraestructura > Defensa del perímetro > Reglas y filtros de cortafuegos	Continúe implementando cortafuegos u otros controles de acceso de nivel de red en todas las ubicaciones de oficinas, realice pruebas con frecuencia y verifique que todos los cortafuegos funcionan correctamente.
Infraestructura > Autenticación > Cuentas inactivas	Visite con regularidad los sitios de fabricantes y otros proveedores de soluciones de seguridad para buscar avisos de ataques recientes y brotes de virus Realice auditorías regularmente para comprobar que los usuarios remotos actualizan sus sistemas. Trabaje conforme a las mejores prácticas recomendadas.
Prioridad baja	
Infraestructura > Defensa del perímetro > Antivirus - Equipos de escritorio	Continúe con la práctica. Utilice una directiva que requiera a los usuarios a actualizar las firmas de virus. Piense en añadir el cliente antivirus al entorno predeterminado de creación de estaciones de trabajo.

Infraestructura > Defensa del perímetro > Antivirus - Servidores	Continúe con la práctica. Plantéese controlar activamente los clientes antivirus de los servidores desde una consola de gestión central para la utilización de configuraciones y firmas de virus. Si utiliza Microsoft Exchange, considere emplear las funciones adicionales de antivirus y los filtros de contenidos para los buzones de correo.
Aplicaciones > Diseño de aplicaciones > Autorización y control de acceso	Piense en probar exclusivamente las aplicaciones principales que procesen datos confidenciales y las interfaces disponibles para los usuarios por Internet. Incluya pruebas tipo "caja negra" e "informadas" de la aplicación y compruebe la asignación de mayores privilegios.
Operaciones > Directiva de seguridad > Regulación	Continúe desarrollando y ejecutando directivas para normativas del entorno informático, de acuerdo con los estándares de aplicación (ISO17799, CoBIT, HIPAA, SOX, etc.)
Operaciones > Directiva de seguridad > Directiva de seguridad	Continúe con el uso de la directiva de seguridad de información, pero revísela y actualícela de forma periódica para reflejar los cambios tecnológicos y del entorno.

Apéndices

Preguntas y respuestas

Las siguientes respuestas se proporcionaron como entrada en esta evaluación.

Cuestión de la evaluación	Su respuesta
Perfil de riesgos para la empresa (BRP)	
Número de equipos de escritorio y portátiles que se utilizan en su empresa:	Entre 150 y 299
Número de servidores que se utilizan en su empresa:	Más de 25 servidores
¿Tiene su empresa una conexión permanente a Internet?	Sí
¿Acceden los clientes y fabricantes a su red o sistemas internos a través de Internet?	Sí
¿Alberga su empresa algunos servicios de aplicaciones externas, como por ejemplo, un portal o un sitio Web, para sus socios o clientes externos?	Sí
¿Dispone su empresa de servicios que usen los clientes internos y externos en el mismo segmento de red?	Sí
¿Se conectan directamente los socios o clientes externos a los sistemas internos de la aplicación para acceder a los datos, actualizar los registros o gestionar de cualquier otra forma la información?	No
¿Se utilizan los mismos componentes de infraestructura de aplicación, como por ejemplo, bases de datos en apoyo de las aplicaciones externas y los servicios corporativos internos?	Sí
¿Permite su empresa que los empleados o los contratistas accedan remotamente a la red corporativa interna?	Sí

¿Se permite que los empleados puedan utilizar sistemas que no sean de producción en la red corporativa general, como por ejemplo, servidores Web personales o equipos que actúen como hosts de "proyectos personales"?	No
Aparte de los dispositivos de cinta y de copia de seguridad, ¿permite su empresa procesar la información confidencial o de propiedad fuera de las instalaciones?	No
En el caso de que los sistemas de seguridad se vieran comprometidos, ¿afectaría ello significativamente la capacidad comercial de su empresa?	No
¿Comparte su empresa espacio de oficinas con otras entidades?	Sí
¿Se desarrollan aplicaciones en su empresa?	Sí
¿Permite su empresa que los desarrolladores de software se conecten de forma remota a los recursos de desarrollo corporativos o que desarrollen remotamente código para aplicaciones?	No
¿Desarrolla o pone en venta su empresa algunos productos de software para el uso de clientes, socios o el mercado en general?	No
¿Se permite que los desarrolladores prueben o desarrollen los sistemas en sitios remotos o inseguros?	No
¿Actúa el personal de TI como guardianes (en contraposición a los desarrolladores) de la línea de aplicaciones comerciales?	No
Según los procedimientos de su empresa, ¿es necesario la actuación de un tercero para almacenar, procesar o distribuir los datos?	No
¿Se almacenan o procesan los datos del cliente en un entorno compartido con los recursos corporativos?	Sí
¿Recurre a fabricantes independientes de software para complementar la oferta de servicios empresariales?	Sí
¿Obtiene su empresa ingresos por ofrecer servicios que incluyen el procesamiento o la minería de datos?	No
Los datos que procesan las aplicaciones de su empresa, ¿se consideran confidenciales o vitales para las operaciones comerciales de sus clientes?	Sí
¿Se ofrecen aplicaciones comerciales críticas a través de conexiones a Internet?	No
¿Quiénes son los usuarios objetivos de las aplicaciones principales de su entorno?	Empleados internos y clientes, fabricantes y socios externos
¿Cómo acceden los usuarios a las aplicaciones principales?	Tanto desde la red interna como de forma remota
¿Está conectada su red corporativa a otras redes (ya sean de clientes, de socios o de terceros) mediante enlaces de red públicos o privados?	Sí
¿Obtiene su empresa ingresos por servicios basados en el almacenamiento o la distribución electrónica de datos, como por ejemplo, archivos de medios o documentación?	No
En los últimos seis meses, ¿se ha sustituido radicalmente algún componente tecnológico de gran importancia?	No

¿La actividad de su empresa depende de la recepción o el procesamiento de datos por parte de socios, fabricantes o terceros?	Sí
Un incidente que afecte a las aplicaciones o a las infraestructuras orientadas a los clientes, como un apagón o el fallo de una aplicación o hardware, ¿afectaría significativamente a sus ingresos?	Sí
¿Almacena su empresa datos confidenciales de sus clientes o de importancia vital?	Sí
Los componentes de infraestructura y las aplicaciones del cliente, ¿dependen del acceso a recursos de su entorno?	No
¿Comparte su empresa los componentes de infraestructura y aplicaciones entre varios clientes?	No
¿Considera que los recursos de TI son un requisito para su empresa?	Sí
¿Utilizan todos los empleados de su empresa equipos informáticos para desarrollar su trabajo?	No
¿Subcontrata su empresa el mantenimiento o la propiedad de alguna parte de su infraestructura?	Sí
¿Tiene su empresa algún plan a medio o largo plazo para la selección y utilización de componentes de nuevas tecnologías?	No
¿Cree que su empresa participa en la adopción rápida de las nuevas tecnologías?	No
¿Selecciona e implanta su empresa nuevas tecnologías basadas en acuerdos de licencias y asociaciones existentes?	No
¿Limita su empresa las opciones relacionadas con la tecnología a aquellas que conoce actualmente el personal de TI?	Sí
¿Amplía su empresa su red mediante la adquisición de nuevas empresas con sus entornos correspondientes?	No
¿Permite su empresa que los empleados descarguen a sus estaciones de trabajo datos corporativos o datos confidenciales de los clientes?	Sí
¿Limita su empresa el acceso a la información en función de los roles de los usuarios?	Sí
¿Implanta su empresa nuevos servicios o aplicaciones antes de evaluar los posibles riesgos para la seguridad?	No
¿Cambia su empresa periódicamente las credenciales de las cuentas con privilegios?	No
¿Cambia su empresa las credenciales de las cuentas con privilegios cuando el personal deja de trabajar en la empresa?	No
Seleccione la opción que mejor defina el sector profesional de su empresa:	Fabricación (discreto)
Seleccione el número de empleados de su empresa:	Entre 150 y 299 empleados
¿Su empresa tiene más de una oficina?	Sí
¿La actividad de su empresa se desarrolla en un mercado de gran competencia o de investigación, en el que el robo de material	Sí

intelectual o el espionaje son temas de gran preocupación?	
¿Cambia muy a menudo el personal técnico en su empresa?	Sí
¿Los productos o las marcas de su empresa tienen reconocimiento?	Sí
¿Utiliza su empresa versiones obsoletas de software que ya no cuenten con el servicio técnico del fabricante?	Sí
¿Adquiere su empresa el software de fabricantes o proveedores conocidos y fiables?	No
Infraestructura	
¿Utiliza su empresa cortafuegos u otros controles de acceso en los perímetros de la red para proteger los recursos corporativos?	Sí
¿Aplica su empresa estos controles en todas las oficinas?	Sí
¿Utiliza su empresa una zona neutral (normalmente conocida como 'zona desmilitarizada' o DMZ) para separar las redes internas y externas de los servicios albergados?	No
¿Alberga su empresa servicios relacionados con Internet en la red corporativa?	No
¿Utiliza su empresa software de cortafuegos basado en hosts para proteger los servidores?	Sí
¿Utiliza su empresa hardware o software de detección de intrusiones para identificar los ataques a la seguridad?	No
¿Se utilizan soluciones antivirus en el entorno?	Sí
Seleccione los sistemas que utilizan soluciones antivirus:	Servidores de correo electrónico Hosts del perímetro (pasarelas, proxies, relés, etc.) Equipos de escritorio Servidores
¿Se puede acceder a la red de la empresa de forma remota?	Sí
Seleccione quién se puede conectar a la red de forma remota:	Empleados Contratistas Terceros, como fabricantes, socios o clientes
¿Se utiliza la tecnología de red privada virtual (VPN) para la conectividad segura a los recursos corporativos de los usuarios remotos?	No
¿Se utiliza autenticación multifactor (token o tarjeta inteligente, etc.) para los usuarios remotos?	No
¿Tiene la red más de un segmento?	Sí
¿Se segmenta la red para separar los servicios de clientes externos y servicios extranet de los recursos corporativos?	No
¿Dispone la red de opciones de conexión inalámbrica?	Sí
¿Cuáles de los siguientes controles de seguridad se usan para regular las conexiones a las redes inalámbricas?	Cambio del nombre de red predeterminado/predefinido (conocido también como Identificador del conjunto de servicio o SSID) del punto de acceso Activar Acceso protegido de fidelidad inalámbrica (WPA) Activar restricciones de dirección por hardware (también conocido como Control de acceso al medio, o MAC)

¿Existen controles para hacer cumplir las directivas de contraseñas en todas las cuentas?	No
¿Su organización dispone de procesos para revisar cuentas administrativas inactivas, de uso interno, de proveedor y de usuario remoto?	No
¿Es su empresa la que configura los sistemas o esta tarea la efectúan otros proveedores o revendedores de hardware?	Configurado por personal interno
¿Cuáles de los siguientes elementos se han creado basándose en una configuración documentada o en una simulación formal?	Ninguno
¿Cuáles de las soluciones siguientes se han instalado en las estaciones de trabajo y los portátiles de los empleados?	Software de gestión/control remoto Protector de pantalla protegido por contraseña
¿Su organización cuenta con procedimientos de respuesta ante incidentes formales?	No
¿Se han aplicado controles de seguridad físicos para garantizar la seguridad de los activos de la empresa?	Sí
¿Cuáles de los siguientes controles de seguridad se utilizan?	Equipos de red (conmutadores, cableado, conexión a Internet) en habitaciones cerradas con acceso restringido Los equipos de red se encuentran además en un armario cerrado Los servidores están en una habitación cerrada con acceso restringido Los servidores se hallan también en armarios cerrados
¿Cuáles de los siguientes controles de acceso físico se utilizan?	Tarjetas de identificación para empleados y visitantes Registros de visitantes Controles de entrada
Aplicaciones	
¿Dispone su empresa de una línea de aplicaciones comerciales (LOB)?	No
¿Utiliza macros personalizadas para las aplicaciones de Office (como, por ejemplo, Word, Excel o Access)?	No
¿Qué mecanismos tiene su empresa para asegurar una disponibilidad alta de las aplicaciones? Seleccione los mecanismos utilizados de la lista siguiente:	Ninguno
¿Ha desarrollado un equipo interno de desarrollo algunas de las aplicaciones principales de su entorno?	Sí
¿Proporciona con regularidad el equipo de desarrollo interno las actualizaciones de software y seguridad, así como la documentación sobre los mecanismos de seguridad?	No
¿Los consultores/proveedores de terceros han desarrollado alguna aplicación clave implementada en su entorno?	Sí
¿El consultor/proveedor de terceros proporciona actualizaciones de software, revisiones de seguridad y documentación sobre mecanismos de seguridad? (sigue siendo compatible)	Revisión final
¿Proporcionan con regularidad los fabricantes independientes las actualizaciones de software y seguridad, así como la documentación sobre los mecanismos de seguridad? (todavía se admite)	No
¿Qué metodologías de desarrollo de seguridad de software se	Ninguna

practican en su empresa? (Seleccione todas las respuestas que correspondan)	
¿Conoce su empresa las vulnerabilidades de seguridad que existen actualmente en las aplicaciones de su entorno?	No
¿Su empresa proporciona formación sobre seguridad para el personal de desarrollo y pruebas?	No
¿Su empresa confía en herramientas de software como parte del proceso de prueba y auditoría para el desarrollo de software seguro?	Sí, para algunos proyectos
¿Existen controles para hacer cumplir las directivas de contraseñas de las aplicaciones principales?	No
¿Tienen las aplicaciones principales del entorno mecanismos para limitar el acceso a los datos y las funciones confidenciales?	Sí
¿Guardan las aplicaciones principales del entorno mensajes en archivos de registro para su análisis y auditoría?	Sí
Seleccione los tipos de eventos que se registran:	Intentos de autenticación fallidos Autenticaciones correctas Errores de la aplicación Acceso a recursos denegado Acceso a recursos permitido
¿Las aplicaciones utilizadas validan los datos de entrada?	No
¿Cifran las aplicaciones principales los datos confidenciales y críticos de la empresa que se encargan de procesar?	No
Operaciones	
¿Es la empresa la que gestiona el entorno o se contrata los servicios de un tercero?	La empresa gestiona el entorno
¿Utiliza la empresa hosts de gestión dedicados a la administración segura de los sistemas y dispositivos del entorno?	No
¿Se utilizan cuentas de registro individuales para las actividades normales en contraposición con las actividades administrativas o de gestión?	Sí
¿Garantiza la empresa a los usuarios el acceso administrativo a sus estaciones de trabajo y equipos portátiles?	No
¿Se comprueba periódicamente el cortafuegos para garantizar que funciona según lo previsto?	No
¿Su organización mantiene planes de recuperación ante desastres y de reanudación de negocio?	No
¿Existe un modelo para asignar niveles de importancia a los componentes del entorno informático?	Sí
¿Existen directivas para la regulación del entorno informático?	Sí
¿Existe una directiva de seguridad de información para la regulación de la actividad relacionada con la seguridad en la empresa?	Sí
Indique quién desarrolló la directiva:	Sólo el departamento de TI
¿Hay una directiva corporativa para el uso aceptable?	No

¿Hay directivas para la gestión de las cuentas de usuarios individuales?	No
¿Hay un proceso documentado para la creación de hosts? Si la respuesta es afirmativa, ¿de qué tipo? (¿Para qué tipos de hosts hay un proceso de creación documentado?)	Ninguno
¿Hay pautas documentadas que indiquen qué protocolos y servicios están permitidos en la red corporativa? Seleccione la opción adecuada:	No hay directivas
¿Su organización dispone de un proceso formal bien documentado para la eliminación de datos en medios electrónicos y en formato impreso?	No
¿Su organización dispone de un esquema de clasificación de datos con directrices de protección de datos asociadas?	No
¿Hay un proceso de gestión para las configuraciones y los cambios?	No
¿Existe un proceso establecido para las directivas de actualización y revisión?	No
¿Existe una directiva establecida por la que se regule la actualización de productos de detección basados en firmas?	Antivirus
¿Hay diagramas lógicos y documentación de configuración precisa para la infraestructura de red y los hosts?	No
¿Existen diagramas exactos de la arquitectura y del flujo de datos de las aplicaciones principales?	No
¿Está activado en el entorno el registro de los eventos producidos en los hosts y los dispositivos?	No
¿Se hacen copias de seguridad de todos los recursos críticos y confidenciales periódicamente?	No
Personal	
¿Hay en su empresa individuos o grupos que sean responsables de la seguridad?	Sí
¿Tienen estos individuos o grupos experiencia en el tema de la seguridad?	Sí
¿Estos individuos o grupos se ocupan de establecer los requisitos de seguridad de las tecnologías nuevas y existentes?	Sí
¿En qué etapa del ciclo de vida de la tecnología suele participar este equipo o individuo encargado de la seguridad?	Planificación y diseño Implantación Pruebas Utilización
¿Existen responsabilidades y roles definidos para cada individuo que participa en la seguridad de la información?	Sí
¿Realiza su empresa evaluaciones de la seguridad del entorno a través de terceros?	No
¿Realiza su empresa evaluaciones de la seguridad del entorno de forma interna?	No
¿Realiza la empresa comprobaciones del historial personal como parte del proceso de contratación?	Sí

Seleccione la opción más adecuada:	Se hacen comprobaciones del historial personal de cada aspirante
¿Hay un proceso formal para la salida de la empresa de los empleados?	No
¿Hay una directiva formal para las relaciones con terceros?	No
¿Hay un programa de divulgación de las medidas de seguridad en su empresa?	No
¿Se ofrece a los empleados formación relacionada con el cargo que desempeñan en la empresa?	No

Glosario

El glosario presenta los términos y conceptos estándar en el sector de las soluciones de seguridad mencionados en este informe. También se pueden incluir términos adicionales que no se encuentran en este informe.

Término	Definición
AoAs	Áreas de análisis que son la infraestructura, las aplicaciones, operaciones, y la gente.
Aplicaciones	Software informático que proporciona funcionalidad al usuario final. Requiere la existencia de un sistema operativo en el que ejecutarse. Algunos ejemplos son los procesadores de texto, las hojas de cálculo o los programas de gestión de bases de datos.
Antivirus (AV)	Software o tecnología de hardware que protege al entorno informático frente a cualquier software peligroso.
Perfil de riesgos para la empresa (BRP)	Medida del riesgo al que está expuesto una empresa, según el entorno empresarial y el sector en que compite.
Índice de defensa en profundidad (DiDI)	Medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una empresa.
Zona desmilitarizada (DMZ)	Parte de la red separada de la red interna mediante un cortafuegos y conectada a Internet a través de otro cortafuegos.
Servidor de seguridad (cortafuegos)	Dispositivo de hardware o software que ofrece protección a los equipos frente al acceso no autorizado a través de la red.
Infraestructura	Funcionalidad de red, así como su administración y mantenimiento para ofrecer compatibilidad con la defensa de red, respuesta frente a incidentes, disponibilidad de red y análisis de errores. Incluye compatibilidad con los procesos empresariales internos y externos, y acerca de cómo se crean e implementan los hosts.
Autenticación multifactor	Autenticación que requiere una combinación de al menos dos de los siguientes elementos: algo que se sabe; algo que se tiene; o algo propio del usuario. Por ejemplo, la tarjeta de débito de su banco es una autenticación de dos factores: requiere algo que tiene (la tarjeta) y algo que sabe (el número PIN). Solicitar a alguien que teclee múltiples contraseñas para la autenticación, supone una autenticación de un solo factor al tratarse únicamente de algo que sabe el usuario. Por lo general, cuantos más factores, más segura es la autenticación. Así, un sistema que requiera un tarjeta identificativa (algo que posee), un PIN (algo que sabe) y una huella dactilar escaneada (algo propio) es más seguro que cualquier otro que únicamente solicite el nombre de usuario/ contraseña (factor único) o una tarjeta de identidad y el PIN.

Operaciones	Los miembros de una empresa, así como las directivas, los procesos, los procedimientos y las prácticas que se relacionan con su protección y la de la empresa.
Personal	Los miembros de una empresa, así como las directivas, los procesos, los procedimientos y las prácticas que se relacionan con su protección y la de la empresa.
Infraestructura de clave pública (PKI)	Conjunto integrado de tecnologías necesario para proporcionar un cifrado por clave pública y firmas digitales. Utiliza una combinación de cifrado por clave pública y privada que ofrece gestión de claves e integridad y confidencialidad de los datos.
Proceso	Serie documentada de tareas secuenciales que se utiliza para realizar una función del negocio.

Interpretación de gráficos

- La puntuación del BRP va de 0 a 100. Una puntuación más alta significa un riesgo posible aumentado al que está expuesta su empresa en esta área de análisis. Es importante tener en cuenta que una puntuación de 0 no es posible; dedicarse a una actividad comercial siempre implica un nivel de riesgo. También es importante comprender que hay riesgos comerciales que no se pueden mitigar directamente.

- DiDI también tiene una puntuación de 0 a 100. Una puntuación más alta significa un entorno donde han tomado más medidas para implementar estrategias de DiD en el área de análisis específica. La puntuación DiDI no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno.

- En principio, una puntuación baja del BRP y alta del DiDI parecería un buen resultado, pero no siempre es así. Está fuera del ámbito de la presente autoevaluación tener en cuenta todos los factores. Una disparidad significativa entre la puntuación del BRP y la del DiDI para un área de análisis específica significa que se recomienda una revisión del área. Cuando analice sus resultados, es importante tener en cuenta las puntuaciones individuales, tanto de BRP como de DiDI, y cómo se relacionan entre sí. Un entorno estable probablemente tendría como resultado puntuaciones iguales en todas las áreas. Disparidades entre las puntuaciones DiDI son un indicio de una estrategia general de seguridad concentrada en una sola técnica de mitigación. Si la estrategia de seguridad no abarca el personal, los procesos ni la tecnología, el entorno estará expuesto a un mayor riesgo de ataque.