

# Anexo I

## Ámbitos Cubiertos

## **1. Introducción**

El presente anexo resume los principales ámbitos y requerimientos contenidos en el documento denominado “Procedimientos Operacionales y de Seguridad”, aprobado el Ministerio, los que deben ser íntegramente cumplidos por el interesado.

Dado que dichos requerimientos inciden en la seguridad del sistema del Medio de Acceso, el documento mismo será entregado sólo a quienes hayan firmado previamente el respectivo acuerdo de confidencialidad.

En consecuencia, el presente anexo tiene carácter meramente descriptivo para que los interesados puedan hacerse una idea de los ámbitos y requerimientos definidos por el Ministerio, siendo obligación de los interesados ajustarse al documento “Procedimientos Operacionales y de Seguridad” en su totalidad.

## **2. Ámbitos considerados**

### **2.1 Definición de la arquitectura de la información**

La empresa candidata debe contar con una arquitectura de información, en la cual se identifique detalladamente la función de los sistemas de información relacionados en mayor o menor medida con el proceso de producción de medios de acceso, acorde a los estándares de seguridad requeridos por Metro.

Este modelo de arquitectura de la información toma en consideración: Repositorio automatizado de datos, reglas de sintaxis de datos, propiedad de la información y clasificación con base en criticidad/seguridad, un modelo de información que represente el negocio, estándares de arquitectura de información de la empresa, operatividad de las acciones, sustentado en procedimientos y normas aprobadas y apoyadas por la dirección.

### **2.2 Definición de la organización y de las relaciones de TI**

La organización TI del candidato se debe definir tomando en cuenta los requerimientos de personal, funciones, delegación, autoridad, controles, roles, responsabilidades y supervisión. La organización estará incrustada en un marco de trabajo de procesos de TI, que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio en el control y toma de decisiones. Deben existir procesos, políticas administrativas y procedimientos formales, vigentes, autorizados y divulgados, para todas las funciones, con atención específica en el control, el aseguramiento de la calidad de los procesos TI, la administración de riesgos, la seguridad de la información, el control de cambio, la propiedad de datos y de sistemas, la segregación de tareas y la integridad de la información. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.

### **2.3 Comunicación de los objetivos y aspiraciones de la gerencia**

La dirección de la empresa candidata debe elaborar un marco de trabajo de control empresarial para TI, definir y difundir las políticas. Deberá implantar un programa de comunicación continua para articular la misión, los objetivos de servicio, las políticas y procedimientos, aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concientización y el entendimiento de los riesgos de negocio y de TI. Dentro del proceso de

comunicación de objetivos y aspiraciones de la gerencia, se deben garantizar, en todo momento, el cumplimiento de las leyes y reglamentos relevantes.

#### **2.4 Evaluación y administración los riesgos de TI**

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia.

#### **2.5 Administración de calidad de los procesos TI**

El candidato debe elaborar y mantener un sistema de administración de calidad, que incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de la calidad de los procesos TI, proporcionando requerimientos, procedimientos y políticas claras de calidad de dichos procesos. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.

#### **2.6 Adquisición y mantenimiento de software de aplicación**

Las aplicaciones del candidato deben estar disponibles de acuerdo a los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad de Metro, el desarrollo y la configuración de acuerdo a los estándares exigidos. Esto permite a la organización apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctamente, todos los puntos tratados en este ítem del documento son requeridos de acuerdo al modelo de madurez por el cual la empresa se rija (mínimo CMM-CMMI nivel 2), y de acuerdo al modelo de desarrollo utilizado, el cual debe ser conocido y aprobado por Metro, con el fin de asegurar la seguridad en cada uno de los subprocesos de construcción de software.

#### **2.7 Adquisición y mantenimiento de la arquitectura tecnológica**

El candidato debe contar con procesos para adquirir, implantar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

#### **2.8 Administración de Cambios**

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar, previo a su desarrollo e

implantación, y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

## **2.9 Instalación y acreditación de soluciones y cambios**

Tiene como objetivo controlar la instalación y acreditación de sistemas, verificar y confirmar que la solución sea adecuada para la producción de los medios de acceso. Esto debe realizarse mediante una migración de instalación, conversión y plan de aceptación adecuadamente formalizado y aprobado por Metro.

Se deben tener en cuenta los siguientes aspectos: capacitación de los usuarios y del personal de operaciones de TI, conversión de datos, un ambiente de pruebas seguro que refleje el ambiente real, acreditación, revisiones y retroalimentación y post implementación, usuario final involucrado en las pruebas, planes continuos de mejoramiento de calidad, requerimientos de continuidad del negocio, mediciones de rendimiento y capacidad, criterios de aceptación previamente acordados.

## **2.10 Garantía de la continuidad del servicio**

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenamiento de forma periódica, basado en los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

## **2.11 Garantía de la seguridad de sistemas**

La necesidad de mantener la confidencialidad, integridad y disponibilidad de la información, y de los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

## **2.12 Educación y entrenamiento a los usuarios**

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requiere identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave, tales como las medidas de seguridad de los usuarios.

## **2.13 Administración de datos**

Una efectiva administración de datos, requiere de la identificación de requerimientos de datos. El proceso de administración de información, incluye el establecimiento de procedimientos efectivos para administrar la biblioteca de medios, el respaldo, la recuperación de datos y la eliminación

apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

#### **2.14 Administración del ambiente físico**

La protección de los equipos de cómputo (Terminales, Servidores, HSM), del personal y de los activos físicos, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico, incluye la definición de los requerimientos del centro de datos (site), áreas de proceso y bodegas (tarjetas producidas y mermas), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

#### **2.15 Definición y Administración de Niveles de Servicios (SLA)**

Define una comprensión común del nivel de servicio requerido, el cual se hace posible a través del establecimiento de acuerdo de niveles de servicio, que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio.

### **3. Alcance de los Requerimientos**

A continuación se detallan a nivel general, los principales ítems de la descripción tecnológica de la fábrica, de los cuales se generarán requerimientos contenidos en el documento denominado "Procedimientos Operacionales y de Seguridad", aprobado el Ministerio, los que deben ser íntegramente cumplidos por el interesado.

#### **Definición de la Arquitectura de la Información**

ITEM
Modelo de la arquitectura de la información
Esquema de clasificación de datos
Administración de la integridad
Esquema General de Arquitectura propuesta para la producción de medios de acceso.

#### **Definición de la organización y de las relaciones de TI**

ITEM
Información de la empresa
Roles y responsabilidades

Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
Propiedad de datos y de sistemas
Segregación de funciones
Supervisión
Administración de políticas para TI
Implantación de políticas de TI

**Evaluación y administración los Riesgos de TI**

ITEM
Identificación de eventos
Evaluación de riesgos
Respuesta a los riesgos

**Administración de la calidad de los procesos TI**

ITEM
Estándares de desarrollo y de adquisición
Método de diseño
Cambios significativos a sistemas actuales
Definición y documentación de requerimientos de archivos
Definición de interfaces
Pruebas al software de aplicación
Evaluación de nuevo hardware y software
Mantenimiento preventivo para hardware
Seguridad del software de sistema
Mantenimiento del software de sistema
Controles para cambios del software de sistema

Uso y monitoreo de utilidades / Utilitarios del sistema

**Administración de Cambios**

ITEM
Control de cambios
Documentación y procedimientos
Distribución de software

**Instalación y acreditación de soluciones y cambios**

ITEM
Metodología de ciclo de vida de desarrollo de sistemas
Entrenamiento de usuarios y pruebas de desarrollo
Reportes de estatus y post-implementación

**Garantía de la continuidad del servicio**

ITEM
Marco de referencia de continuidad Operacional
Marco de referencia de continuidad de tecnología de información
Contenido del plan de continuidad de tecnología de información
Mantenimiento del plan de continuidad de tecnología de información
Pruebas del plan de continuidad de tecnología de información
Distribución del plan de continuidad de tecnología de información

**Garantía de la seguridad de sistemas**

ITEM
Administrar medidas de seguridad
Identificación, autenticación y acceso
Administración de cuentas de usuarios

Revisión general de cuentas de usuario
Control de usuarios sobre cuentas de usuario
Clasificación de datos
Administración centralizada de identificación y derechos de acceso
Reportes de violación y de actividades de seguridad
Manejo de incidentes
Confianza en las contrapartes
Comunicación segura, cifrado de canales
Protección de las funciones de seguridad
Resguardo y Administración de las llaves criptográficas y registro básico (mapping) (HSM)
Prevención, detección y corrección de software malicioso
Identificación de necesidades de entrenamiento
Organización de entrenamiento
Entrenamiento sobre principios y conciencia de seguridad

**Administración de datos**

ITEM
Manejo de errores en la entrada de datos
Integridad de procesamiento de datos
Manejo y retención de datos de salida
Distribución de datos de salida
Provisiones de seguridad para reportes de salida
Protección de información sensible durante transmisión y transporte
Protección de información sensible a ser desechada

**Administración del ambiente físico**

ITEM
Seguridad física (cctv, control de acceso, entre otros)
Discreción (bajo perfil) y seguridad de las instalaciones de tecnología de información
Escolta de visitantes
Protección contra factores ambientales

**Definición y Administración de Niveles de Servicios (SLA)**

Item
Marco de Referencia para los acuerdos de Nivel de Servicio
Monitoreo y Reporte
Fabricación de Tarjetas
Mermas