Ministerio de Modernización
Presidencia de la Nación

Relevamiento de Data Centers

Requerimiento de Información

Dirección Nacional ONTI

Julio 2016

Histórico de Revisiones

Revisión	Descripción del Cambio	Actualizado por	Fecha
0.1	Creación del documento		
0.2	Revisión y actualización		
0.3	Revisión		

TABLA DE CONTENIDO

1. MAPA DE INFRAESTRUCTURA Y EQUIPAMIENTO:

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Relevamiento de arquitectura física end-to-end incluyendo: *- servidores*	1. Inventario Servidores Físico a. N° b. Rack c. Blade d. Chasis e. Marca f. Marca y modelo Procesador g. Capacidad utilizada de discos o capacidad disponible en discos h. Harddrive (Cant. Discos) i. Total GB en uso j. S.O. k. Organismo l. Nombre m. Estado n. Checkmark o. Comentarios 2. Inventario Servidores Lógico a. Nro Servidor b. Rol Máquina Virtual c. Versión Sistema operativo d. Detalles o comentarios a tener en cuenta 3. Otros a. Cantidad de servidores que posee el Organismo a la fecha. b. Cantidad de servidores apagados o fuera de producción. c. Detallar existencia de servidores en desuso que estén pronto a ser utilizados o puestos en producción.	
Relevamiento de arquitectura física end-to-end incluyendo: *- dispositivos de comunicaciones*	Inventario Equipos DC 1. N° 2. Rack 3. Marca 4. Modelo 5. Puertos 6. Rol 7. Checkmark 8. Comentarios 9. Dispositivos redundantes Inventario Equipos de Seguridad y otras aplicaciones del DC (FW, IDS, Balanceadores de Carga) 1. N° 2. Rack 3. Marca	

	4. Modelo 5. Puertos 6. Rol 7. Checkmark 8. Comentarios 9. Dispositivos redundantes Inventario de Equipos Networking Edificio (Switches de Piso) 1. N° 2. Rack 3. Marca 4. Modelo 5. Puertos 6. Rol 7. Checkmark 8. Comentarios 9. Dispositivos redundantes Inventario de Equipos Networking WI-FI Edificio (APs, WLC) 1. Rack 2. Marca 3. Modelo 4. Puertos 5. Rol 6. Checkmark 7. Comentarios 8. Dispositivos redundantes	
Relevamiento de arquitectura física end-to-end incluyendo: *- dispositivos de almacenamiento*	1. N° 2. Marca 3. Modelo 4. Hostname 5. Capacidad total 6. Capacidad actual utilizada 7. Checkmark 8. Dirección IP 9. Soporte del fabricante Comentarios	
Relevamiento de arquitectura física end-to-end incluyendo: *- dispositivos de copias de respaldo*	1. Indicar qué tipo de dispositivos de copias de resguardo se utilizan. 2. Capacidad de almacenamiento total tienen 3. Capacidad de almacenamiento poseen los equipos al día de hoy 4. Indicar cómo se realizan los cambios de Cinta (manual o automático) 5. Características posee la librería física 6. Características posee la librería virtual	
Procedimiento de Gestión de	1. Procedimiento escrito para la gestión de cambios en infraestructura a. Segregación de roles	

Cambio en Infraestructura	b. Separación de ambientes c. Pruebas 2. Documento que detalle el Capacity Plan, Monitoring Plan, Management Plan, etc.	
Aspectos existentes para disponibilidad	1. Detallar tanto a nivel documental, infraestructura o configuración, la disponibilidad de los activos de información.	
Aspectos existentes para medir/controlar la performance	1. Reportes de performance en las comunicaciones. 2. Reportes de performance en el procesamiento. 3. Reportes de performance en transferencia de información, etc. 4. Detallar para los puntos anteriores procesos, políticas e implementaciones definidas.	
Herramientas y procesos para el monitoreo y control	1. Listar las herramientas utilizadas para el monitoreo y control, detallando: d. Nombre. e. Versión. f. Tipo de uso que se le da al aplicativo. g. Comentarios acerca del aplicativo. h. Soporte del Fabricante. 2. Procedimiento escrito para el monitoreo y control de infraestructura	
Contratos de Soporte Técnico	1. Contratos de Soporte Técnico y/o Mantenimiento de Hw (Por ej Mantenimiento de Servidores) 2. Contratos de Soporte Técnico y/o Mantenimiento de SW, Licenciamiento (Por ej VMWare ESX, Firewalls virtualizados, etc) 3. Contratos de Soporte Técnico y/o Mantenimiento de RRHH / Serv Prof. 4. Personal Externo Contratado	

2. MAPA DE RED DE COMUNICACIONES:

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Mapa de Red	1. Identificación de cada una de las redes y su funcionalidad (DMZ, VLANs, Red Datacenter, MPLS, TLS, Radio enlaces) 2. Topologías a. Red de Comunicaciones DC b. Red de Seguridad y otras aplicaciones del DC (Ej. FW, IPS, Balanceadores de Carga, etc) c. Red de Comunicaciones de Edificio (Switches de Piso) d. Red de Networking Wi-Fi de Edificio e. Red de Accesos VPN f. Enlaces e Interconexión con otros organismos g. Soluciones especiales de conectividad (Ej. NAC, Videoconfefrencia) 3. Segmentación de red 4. Conexiones existentes (WAN/LAN/WIRELESS y Acceso a INET) 5. Detalle de equipos de telecomunicaciones presentes en las topologías	
Segmentación de Red	1. Detalle de VLANs (indicar rango de ip y equipos asociados) 2. Topología de: red LAN, DMZ, red Datacenter.	
Seguridad en Comunicaciones	1. Descripción de el/los Firewalls a. Tipo, marca y modelo de los firewalls utilizados b. Nivel de utilización de recursos del firewall. c. Versión del Firmware del Firewall. (¿Se encuentra actualizado?) d. IP 2. Estadísticas de ataques y/o intentos de DoS registrados 3. Esquemas y herramientas de filtrado de contenidos (Proxy Services) 4. Capacidad de detección de intrusos (IDS/IPS) 5. Tipificación de usuarios 6. Accesos Remotos (Internet / Extranet / Otros accesos externos). 7. Esquemas de antivirus y filtrado de contenido entrante (SPAM) y saliente (Mail / URL filtering). 8. Personal que administra los distintos dispositivos	
Enlaces de comunicación con otros ministerios o centros de cómputos	1. Empresas proveedoras del servicio 2. Descripción (Ancho de banda, redundancia, puntos interconectados 3. Domicilio Punta B 4. Tipos de servicio (ADSL, Fibra óptica, etc.) 5. Servicio Prestado 6. En uso? 7. Disponibilidad de los enlaces (Mensual, Anual)	

3. MAPA DE APLICACIONES Y SERVICIOS DE IT

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Mapa de servicios de TI utilizados por el Ministerio	1. Detallar el mapa de servicios de TI utilizados por el Organismo (Fileserver, Housing de servidores, Hosting, Desarrollo de Aplicaciones, Wifi, correo electrónico, Lync, etc.)	
Inventario de sistemas y aplicaciones de cada Ministerio *Mapa de Aplicaciones utilizados por el Ministerio, con el detalle de cada sistema*	Inventario de Sistemas 1. Detallar Nombre de cada Aplicativo 2. Organismo al que pertenece 3. Descripción del Aplicativo (Para que se utiliza, etc.). 4. Usuarios Internos 5. Usuarios Externos 6. Criticidad 7. Centro de Cómputo 8. Servidor/Cluster donde se encuentra implementado. 9. Máquina Virtual donde se encuentra implementado 10. Definir criticidad medida como Impacto al Gobierno 11. Definir criticidad medida como Impacto al Ciudadano 12. Servidor donde se encuentra alojado: Describir en cuál de los servidores detallados anteriormente se encuentra alojado dicho aplicativo (ya sea físico o virtual). Indicar servidores de producción, testing, desarrollo y contingencia de cada aplicación según corresponda. 13. Hosting Aplicación: Indicar quien la Hostea. Si se encuentra dentro del Ministerio o en lo de un proveedor. Detallar Proveedor. 14. Mantenimiento: Indicar si el mismo es mantenido. Detallar quien lo mantiene (Interno, Externo, Área Usuario, Interno+Externo) 15. Servicios que Afecta: Describir con detalles los servicios que afecta dicho aplicativo. 16. Integración con otros sistemas: Indicar si el aplicativo mantiene relación con otros sistemas de gobierno, su interacción con los mismos, relación entre los datos. 17. Relación con otros Ministerios / Dependencias: Ser lo más claro posible. 18. Capacidad de Almacenamiento: Cuanto Espacio ocupa el aplicativo, lugar de alojamiento, crecimiento mensual/anual. Detallar cualquier información que crea importante sobre el crecimiento. 19. Cantidad de Usuarios: Cantidad de usuarios que utilizan dicho sistema (usuarios internos al Ministerio como internos al mismo). 20. Servicios: Indicar si el sistema dispone de Servicios (Apis) para integración con otros sistemas. 21. Arquitectura: Arquitectura principal utilizada para la construcción del sistema (Symfony, Java, .NET, SAP, etc.). 22. Canales: Canales utilizados por el sistema (Web, Terminal,	

	Desktop, Mobile, etc.). 23. Lenguaje de programación en el que fue desarrollada la aplicación. 24. En caso de ser de un tercero, indicar y especificar el tipo de contrato que se posee 25. Componentes externos que utiliza la aplicación. 26. Interfaces con otros sistemas: Describir con detalles en caso de que existan interfaces. 27. Url-IP Productivo / Desarrollo / QA: Detallar la URL y la IP de la aplicación en caso que aplique. Describir con detalles cualquier tipo de información importante a considerar. 28. Bases de Datos que utiliza. 29. Describir en éste ítem cualquier información que crea relevante para el correcto funcionamiento de sus aplicativos. 30. Descripción de procedimientos de gestión de cambios en las aplicaciones (escritos o no). 31. Descripción de procesos de desarrollo de aplicaciones (escritos o no). 32. Descripción de ambientes y esquema de segregación actual (Desarrollo, Testing, Producción). Inventario de Software (Visto desde la óptica del usuario. Las apps pueden ser propias o no) 1. Detallar Nombre de cada Aplicativo 2. Descripción 3. Tecnología 4. Año desarrollo 5. Quien lo desarrollo 6. Criticidad 7. Usuarios internos 8. Usuarios externos 9. Centro de Cómputos 10. Soporte Actual? 11. Datos Backup? 12. Contingencia? 13. Criticidad para el Ministerio	
Inventario de Bases de datos de cada Ministerio y su owner	1. Nombre de la Base de datos 2. Aplicación a la que pertenece 3. Servidor físico en el que se encuentra alojada la base de datos 4. Nombre y versión de cada sistema de Administración de Base de Datos (ej. Oracle, SQL Server, DB) 5. IP de la base de datos 6. Licencia: Indicar si la misma cuanta con licencia 7. Centro de Cómputo 8. Owner 9. Procedimientos formales para la realización de cambios en las bases de datos 10. Esquema de autenticación de usuarios que utiliza la base de datos 11. Quién evalúa el riesgo de seguridad de las actualizaciones Describir en éste ítem cualquier información que crea relevante para el correcto funcionamiento de sus bases de	

	datos.	
Procedimientos de gestión de cambios en las aplicaciones	1. Procedimiento de requerimientos y especificaciones técnicas para la instalación de sistemas. 2. Procedimiento de requerimientos y especificaciones técnicas para la realización de cambios a programas. 3. Herramienta utilizada para la realización de los cambios. Detallar: a. Nombre aplicación b. Versión c. Tipo de uso que se le da al aplicativo y funciones que se utilizan del mismo	
Procesos de desarrollo de aplicaciones	1. Procesos formales documentados para el desarrollo de aplicaciones. 2. Describir el equipo de desarrollo existente	
Ambientes y esquema de segregación actual.	1. Descripción de la separación de ambientes existente. 2. Personal dedicado a cada ambiente 3. Indicar si existen servidores dedicados a cada ambiente, y cuáles son. 4. Detallar y/o comentar todos los aspectos relevantes respecto de la segregación de roles y los distintos ambientes de desarrollo	
Herramientas y procesos para el monitoreo y control	1. Herramientas utilizadas para medir el desempeño de las aplicaciones del organismo. 2. Documentación de los procesos llevados a cabo por estas herramientas. 3. Indicar si se monitorea el rendimiento de la infraestructura utilizada por cada aplicativo del organismo. (Servidores donde se aloja la aplicación, redes utilizadas por la aplicación, enlaces utilizados por la aplicación, etc)	
Contratos de Soporte Técnico	1. Contratos de Soporte Técnico y/o Mantenimiento de SW, Licenciamiento (Por ej contrato de licencias de aplicaciones, herramientas de desarrollo de software, SO, Bases de Datos, etc) 2. Contratos de Soporte Técnico y/o Mantenimiento de RRHH / Serv Prof. (Por ejemplo mantenimiento de una base de datos por una empresa externa)	

4. ADMINISTRACIÓN DE LOS ACCESOS LÓGICOS:

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Políticas generales de Seguridad	Proveer las políticas generales de seguridad, y los restantes documentos que conforman el marco normativo de seguridad (normas y procedimientos) relacionados con: 1. Gestión de Incidentes 2. Gestión de Parches y Vulnerabilidades 3. Control de Inventario de Hardware y Software 4. Gestión de Proveedores 5. Gestión de Riesgos 6. Información impresa y formatos equivalentes 7. Personal contratado y terceros 8. Contingencia de la Información 9. Cambios sobre la topología de la red, firewalls y routers 10. Instalación de software 11. Protección física de la Información 12. Políticas de seguridad de la información a. Aprobación formal de alguna autoridad competente b. Detallar si la política se encuentra actualizada 13. Destrucción de información 14. Monitoreo de Servidores, storage, y equipos de comunicaciones: a. Detallar si la misma contempla el Nivel de performance de parámetros de servidores, espacio disponible en disco, etc. 15. Monitoreo de logs de seguridad. 16. Borrado seguro de discos con información sensible 17. Ingreso al Data Center 18. Gestión de usuarios (ABM, Active Directory, etc) 19. Gestión de contraseñas de usuarios 20. Clasificación de la información 21. Clasificación de activos de hardware 22. Clasificación de activos de Software 23. Acceso remoto 24. Licencias de Software 25. Monitoreo de sistemas, login y auditoría. 26. Detallar otras políticas que el Organismo posea. 27. Para las políticas, normas y procedimientos anteriores, indicar: a. Comentarios relevantes respecto de los criterios utilizados en el diseño de las distintas políticas (Aspectos tales como niveles de confidencialidad) b. Porcentaje / grado de implementación del Marco normativo. c. Porcentaje / grado de actualización del Marco normativo.	

Estándares de software de base, herramientas, bases de datos, comunicaciones y seguridad aplicativa	1. Detallar Normas del Marco Normativo (Documentación referente a configuración de servidores a nivel lógico / físico, configuración de dispositivos de comunicación, configuración de clientes, configuración de herramientas de monitoreo y control, etc.) 2. Procedimiento para la administración de Cambios a Programa 3. Procedimiento para la administración de Cambios en Bases de datos	
Procesos existentes para el Alta, baja y modificación de usuarios y perfiles / grupos / etc.	1. Procedimiento para la administración de Altas, Bajas y Modificación de Usuarios.	
Proceso existente para administración de parches de seguridad	1. Procedimiento para la administración de Sistema Operativo (Instalación/Actualización de Parches de Seguridad, Upgrade, etc.)	
Seguridad aplicativa	1. Describir el esquema de autenticación de usuarios de cada uno de los sistemas del organismo 2. Detallar aspectos relevantes respecto a la seguridad aplicativa de los sistemas utilizados por el organismo	
Seguridad lógica del software de base existente	1. Indicar si el organismo posee una solución centralizada de accesos lógicos a los firmwares y sistemas operativos de los servidores. 2. Indicar si el organismo cuenta con software de IDM para la gestión identidades y accesos a los software de base de servidores 3. Documentación sobre quién tiene acceso a cada una de las plataformas que utilizan el parqué de servidores del Data Center	
Responsabilidad sobre los datos.	1. Indicar las responsabilidades definidas de los distintos servicios que ofrece el Datacenter 2. Indicar responsables de cada uno de los servicios que provee el organismo.	
Monitoreo de eventos de seguridad	1. Procedimiento de Monitoreo de Eventos relacionados con seguridad	

Administración de incidentes de seguridad	1. Procedimiento de Gestión de Incidentes de seguridad informática de la infraestructura tecnológica. a. Descripción de la herramienta utilizada para la Gestión de Incidentes, quienes son los operarios, a quienes llegan las notificaciones, cómo se genera la notificación (automática o manual)	
Proceso de clasificación de Información y activos informáticos	1. Describir el proceso de clasificación de información y activos informáticos.	
Proceso de evaluación de riesgos informáticos	1. Descripción de procesos de evaluación de riesgos informáticos. 2. Indicar responsables de realizar la evaluación 3. Indicar qué tipo de evaluación se realiza y sobre qué plataformas y/o servicios.	
Compromisos de confidencialidad y uso de TI para empleados y terceros	1. Detallar si existen controles para asegurar la confidencialidad de los datos y la correcta ejecución de los procesos definidos en las políticas destinadas a tal fin.	
Proceso para la gestión y resguardo de las claves de cuentas de administración de servidores	1. Detallar el proceso de gestión de resguardo de las claves de cuentas de administración de servidores.	

5. OPERACIÓN DIARIA DEL CENTRO DE CÓMPUTOS.

A continuación se detallan los distintos temas a relevar:

Tema	Preguntas Relevamiento	Notas
Existencia del plan de ejecución, su cumplimiento.	1. Indicar si existen procedimientos de planificación y operación de procesos (Por Ej Gestión de Capacidad y Performance, gestión de incidentes, etc) 2. Indicar si existen procedimientos de alta, baja y modificación de procesos	
Verificación de existencia de log de ejecución.	1. Registros de ejecución del proceso (Logs).	
Procedimiento de Implementación de cambios en los distintos ambientes.	1. Descripción del procedimiento de Implementación de cambios en los distintos ambientes	
Identificación de responsables para cada tarea.	1. Listado de responsables para cada tarea.	
Políticas de operación.	1. Descripción de procesos (críticos) funcionales. a. Detalle y descripción del proceso. b. Entradas y salidas. c. Indicar si el proceso se ejecuta de forma manual o mediante un batch. d. Frecuencia de ejecución (diaria, cada 6 horas, etc.) e. Registros de ejecución del proceso (Logs). 2. Descripción de un proceso de evaluación de riesgos de TI y/o riesgos operativos 3. Descripción del proceso de Scheduling de Procesos Batch. 4. Herramienta utilizada para la administración, monitoreo, y control de los procesos diarios. Identificación de los operarios de la herramienta. Detalle de las características de la herramienta.	
Cumplimiento del plan de operación.	1. Describir plan de operación existente. Indicar porcentaje / grado de implementación.	
Impacto por no ejecución de las tareas,	1. Análisis del impacto ante la ejecución incorrecta, o no ejecución, de una tarea. 2. Descripción del proceso de comunicación y solución de incidentes.	
Cuadro de criticidades, y frecuencia de procesamiento de las aplicaciones.	1. Definición de criticidades, y frecuencia de procesamiento de las aplicaciones.	

6. OPERACIONES DE RESGUARDO Y PLAN DE CONTINGENCIA:

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Procedimientos de Backup y Restore actuales	1. Backup – Políticas de Resguardo: Detallar si existe una política de Backup. En caso de existir describir si la misma es diaria, semanal o mensual. Aclarar cualquier información que considere relevante.	
Herramientas y procedimientos utilizados	1. Descripción de la herramienta utilizada para la configuración, monitoreo y control de backups. Indicar administrador responsable. 2. Registros de ejecución de backup (logs).	
Seguridad Física de los medios de resguardo	1. Seguridad física de los medios de resguardo. Dónde se alojan. Quiénes tienen acceso a los mismos.	
Plan de Contingencias.	1. Descripción del proceso de Restore. 2. Existe documentación de pruebas de recupero. 3. Descripción del proceso de Manejo de Contingencias. Comunicación y resolución ante la ejecución incorrecta o no ejecución de backup. 4. Indicar si existe un plan de continuidad de negocio. (BCP). Detallar: Fecha de implementación, fecha de última actualización, quiénes lo aprobaron, documentación de pruebas realizadas.	
Plan de recuperación ante desastres.	1. Indicar si existe un plan formal de recuperación ante desastres. Fecha de implementación, fecha de última actualización, quiénes lo aprobaron, documentación de pruebas realizadas. 2. Identificación de responsables de cada tarea.	

7. ORGANIZACIÓN DE TI

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Organización del área, estructura: - Propia	1. Organigrama específico del área de TI. Cantidad de personas internas y externas de cada sector.	
Organización del área, estructura: - Contratada	1. Listado de personal contratado. Indicar puesto, roles y funciones.	
Organización del área, estructura: - Proveedores	1. Listado de proveedores de tecnología y/o soporte a sistemas. Servicios que ofrece cada proveedor al organismo. 2. Detallar tipo de contrato con cada proveedor, fecha de vencimiento del mismo, y cantidad de licencias. 3. Descripción de políticas de gestión de servicios.	
Roles y las funciones de los grupos de especialistas de IT	1. Documentación de roles y funciones de los integrantes de cada sector del área de TI.	
Compromisos de confidencialidad y uso de TI para empleados y terceros	1. Descripción de convenios, acuerdos, o compromisos de confidencialidad formalmente establecidos con el personal y proveedores. 2. Descripción de convenios, acuerdos, o compromisos formalmente establecidos con el personal y los proveedores acerca del uso responsable de las tecnologías de la información.	
Programa de entrenamiento a personal de TI, y concientización de seguridad a empleados	1. Descripción de cursos de entrenamiento y/o concientización dictados al personal en relación a la seguridad de la información 2. Listado de personal técnico capacitado en plataformas Windows y Linux, Seguridad, Políticas y Procedimientos, y otras disciplinas.	
Organismos descentralizados	1. Detallar los Organismos descentralizados que dependen del Ministerio, indicando: a. Nombre del Organismo descentralizado b. Dirección del Organismo c. La infraestructura que posee (sala de servidores, centro de cómputos, etc.) d. Nombre del responsable de Infraestructura y/o Telecomunicaciones.	
Proyectos IT	1. Proyectos en curso / a futuro de Hardware y/o Software a. Descripción. b. Fecha estimada. c. Criticidad. d. Impacto sobre aplicaciones y/o infraestructura .	
Contratos de Soporte Técnico	1. Contratos de Soporte Técnico y/o Mantenimiento de RRHH / Serv Prof. 2. Personal Contratado	

8. INFRAESTRUCTURA DE CENTRO DE CÓMPUTOS O SALAS DE PROCESAMIENTO:

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Medidas de control de acceso al Centro o Sala de procesamiento	1. Procedimiento de "Seguridad Física de los Recursos Informáticos". 2. Planos de distribución física de los recursos tecnológicos, localizados dentro de los centros de procesamiento de datos. 3. Procedimiento Control de Personal con acceso a los CPD 4. Procedimiento Control Logs - Sistema de Control de Accesos Físico 5. Listado de personal autorizado a acceder al CPD y a sus distintos recintos.	
Medidas de protección ante incendios	1. Diagramas del "Sistema de Extinción del CPD" y de la "Distribución de extintores". 2. Existen controles de mantenimiento periódicos y pruebas sobre el sistema de protección contra incendios. 3. Detallar aspectos de seguridad en la Matriz de Seguridad Física embebida.	
Medidas de protección ante humedad	1. Detalle del sistema de detección de humedad 2. Controles y documentación de mantenimiento periódicos y pruebas sobre el sistema de protección ante humedad 3. Detallar aspectos de seguridad en la Matriz de Seguridad Física embebida.	
Sistemas de energía de emergencia *- Redundancia* *- UPS* *- Generadores*	1. Existen controles y documentación de mantenimiento periódicos y pruebas sobre equipamientos de apoyo en el CPD, tales como, equipos de aire acondicionado, grupos generadores, UPS,etc. 2. Detallar aspectos de seguridad en la Matriz de Seguridad Física embebida.	
Refrigeración *- Principal* *- Respaldo o redundancia*	1. Indicar qué tipo de refrigeración poseen. 2. Equipos de respaldo 3. Indicar si el sistema de refrigeración está diseñado para funcionar las 24hs todo el año 4. Detallar aspectos de seguridad en la Matriz de Seguridad Física embebida.	
Herramientas y procesos para el monitoreo y control	1. Describir herramientas y procesos para el monitoreo y control. 2. Indicar administradores y operadores.	
Contratos de Soporte	1. Contratos de Soporte Técnico y/o Mantenimiento de Hw (Por ej UPS, Aire	

Tema	Información a requerir	Notas
Técnico	Acondicionado, Control ignifugo, Accesos) 2. Contratos de Soporte Técnico y/o Mantenimiento de SW, Licenciamiento (Por ej software de monitoreo) 3. Contratos de Soporte Técnico y/o Mantenimiento de RRHH / Serv Prof. 4. Personal encargado de Mantenimiento	

Agenda de Relevamiento - Segur

9. SISTEMAS COLABORATIVOS

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Comunicaciones Unificadas (servicios de telefonía, mensajería unificada , mensajería instantánea corporativa, conferencias web)	1. El organismo posee una solución de comunicaciones unificadas? 2. Describir la misma. 3. Indicar cantidad de usuarios soportados 4. Planean migrar a una solución de Comunicaciones unificadas? Cuando?	
Mensajería Instantanea	1. Tienen una solución de mensajería instantánea? 2. Describir la misma 3. Indicar cantidad de usuarios soportados 4. Planean migrar a una solución de Comunicaciones unificadas? Cuando?	
Correo Electrónico	1. Qué solución de correo electrónico utiliza el organismo? 2. Indicar Solucion/Version 3. Cantidad de usuarios soportados 4. Describir arquitectura 5. Quien la administra? 6. Quien Soporta? Cuando vence el soporte? 7. Tienen alguna Expansión/mejora planificada para este año? 8. Tienen usuarios fuera del dominio del ministerio utilizando cuentas no oficiales? Cantidad Aproximada?	
Central Telefónica	1. Qué solución de Central Telefónica utiliza el organismo? 2. Indicar Marca/modelo, 3. Cantidad de usuarios Soportados 4. Indicar Tecnología : Analogica/Digital/IP/Hibrida : 5. Describir arquitectura 6. Quien administra? 7. Quien Soporta?.Cuando vence el soporte? 8. Tienen alguna Expansión/mejora planificada para este año?	
Nubes privadas / públicas / híbridas - colaboración	1. El organismo posee una herramienta de colaboración para sus usuarios? 2. Indicar Solucion/Version 3. Indicar arquitectura, 4. Indicar Cantidad de usuarios 5. Utiliza Repositorio? Tamaño en TB? 6. Realiza Colaboración de Aplicaciones (comparte y colabora en documentos)? 7. Planea migrar a una solución de Comunicaciones unificadas? Cuando?	

10. ESQUEMAS DE REDUNDANCIA Y/O RECUPERACIÓN DE DESASTRES

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Redundancia y Recuperación de Desastres	1. Existe hoy un Esquema de Redundancia y/o Recuperación de Desastres para aplicaciones críticas? 2. Describir (Aplicación, Lugar de contingencia, otros datos relevantes) 3. Identifico Aplicaciones críticas que deben contar con un esquema de redundancia y/o R/D 4. Describir (Aplicación y otros datos relevantes)	

11. CUESTIONARIO DE CIBERSEGURIDAD

A continuación se detallan los distintos temas a relevar:

Tema	Información a requerir	Notas
Cuestionario de Ciberseguridad	1. Si cuentan con una política de Seguridad de la Información, si fue aprobada formalmente por una autoridad y si está actualizada. 2. Si cuentan con políticas o procedimientos de clasificación de información, de activos y/o de sistemas y si es asi, en cualquiera de los casos, que criterios utilizan (en base a confidencialidad u otro criterio, 3 o 5 niveles, etc) 3. Si han realizado o realizan algún proceso de evaluación de riesgos de IT u operativos (que contemplen las TI) 4. Si los empleados firman habitualmente convenios, acuerdos o compromisos de confidencialidad y/o de uso responsable de la TI. 5. Si los proveedores o terceros vinculados al Organismo firman habitualmente convenios, acuerdos o compromisos de confidencialidad y/o de uso responsable de la TI. 6. Si tienen algún programa o curso de entrenamiento o concientización en seguridad de la información para los empleados. 7. Cuáles son las capacidades del personal del Area de TI, es decir, si tienen personal técnico entrenado en plataformas Windows, Linux, Seguridad, Políticas y Procedimientos, etc (se podría hacer un punteo de posibles áreas o dejarlo libre para que lo indiquen) 8. Si existen procedimientos formales “protocolos” para la asignación de cuentas y llaves de acceso, para la autorización de accesos a los servidores y para el acceso a las claves de administración. 9. Si las claves de administración de los servidores y dispositivos de red son diferentes de las claves de acceso de usuarios, y si están debidamente documentadas y almacenadas de forma segura fuera del CPD (Política de Resguardo de la Información). 10. Si existen controles para asegurar la confidencialidad de los datos. 11. Si el organismo o la jurisdicción ha adherido al programa Nacional de Infraestructuras Críticas y Ciberseguridad . En caso afirmativo, si los enlaces se encuentran actualizados o caso contrario, si conoce el programa y le interesaría adherir.	