# Oficina de Tecnología
# Plan de Continuidad

***Versión 1.0***
***Diciembre de 2020***

# Tabla de contenido

## 1. Objetivo General

Definir el plan de continuidad de tecnologías de la información de la Unidad de Servicios Penitenciarios y Carcelarios (USPEC) con el fin de establecer las tareas, roles y responsabilidades que permitan restaurar la operación normal de la plataforma tecnológica y los servicios que presta la Oficina de Tecnología de la Entidad.

### 1.1 Objetivos Específicos.

A. Procurar la recuperación de los servicios de tecnología prestados por la Oficina de Tecnología de la entidad, dentro de los márgenes de tiempo tolerables.
B. Minimizar el tiempo de toma de decisiones frente a la recuperación causada por un incidente que haya impactado la continuidad de las actividades que dependen de los servicios de TI de la USPEC.
C. Desarrollar los procedimientos para la respuesta y recuperación ante incidentes o desastres que impacten la prestación de servicios de TI, describiendo las acciones y las responsabilidades que esto con lleva.
D. Mantener el control de las operaciones de TI posterior al desastre, permitiendo el flujo de información sobre el estado de las actividades de recuperación.

## 2. Alcance

Las actividades de recuperación se enmarcan en los servicios tecnológicos prestados por la Oficina de Tecnología a los demás procesos de la entidad y bajo los siguientes aspectos:

- Responsables de los procesos y de las actividades de recuperación
- Tecnología de la Información
- Recuperación de los servicios priorizados de tecnología
- Almacenamiento
- Copias de respaldo (Backups). (Proveedor externo)
- Base de datos
- Control de acceso físico
- Correo electrónico (Proveedor externo)
- DHCP
- DNS
- Equipos de trabajo
- Equipos servidores
- Impresión, copia y digitalización (Proveedor externo)
- Internet (Proveedor externo)
- Monitoreo (Alientvault)
- Controlador de Dominio (AD)
- Telefonía
- Red (Cableada, inalámbrica)
- Antivirus
- Aplicaciones, definidos en el inventario de aplicaciones administrador por la OTEC. Incluye servicios alojados en la nube y localmente.

## 3. Responsables

La Unidad de Servicios penitenciarios y Carcelarios (USPEC) establecerá mecanismos de implementación del Plan de Continuidad de TI mediante la adopción de normas pertinentes y la designación de personal experto encargado de su gestión, estableciendo los mecanismos administrativos, técnicos y procedimentales que se requieran. La responsabilidad en la recuperación de los servicios tecnológicos se encuentra a cargo de:

a. Administradores de la Oficina de Tecnología de los siguientes servicios:

- Servicio de almacenamiento y Backups.
- Administración de las bases de datos.
- Soporte y mantenimiento de los servidores.
- Gestión de redes.
- Monitoreo y seguridad

b. Proveedores de soluciones y servicios de tecnología de la USPEC

- Aplicaciones en la nube.
- Correo Electrónico
- Página Web
- Solución de backup
- Soporte y mantenimiento de los servidores
- Mesa de ayuda
- Servicio de Impresión
- Infodoc.
- MIPGestión
- Canal de internet.
- Servicio de Telefonía

## 4. Actualización

La Oficina de Tecnología es responsable por el mantenimiento y la revisión del Plan de Continuidad de TI.
Se realizará mínimo una revisión anual o las necesarias en respuesta a cualquier cambio que pueda afectar la base original de la evaluación de riesgos, (ej.: cambios de plataforma, nuevos procesos, cambio de estructura organizacional).

## 5. Organización del Plan de Continuidad de TI

### 5.1 Etapas del Plan de Continuidad y responsables

Los desastres tienen tres etapas:

- "Antes" del desastre o incidente.
- "Durante" se asume cuando se actúa o se enfrenta la emergencia a través de los aspectos de Continuidad de Negocio
- "Después" se asocia principalmente al retorno a normalidad y la forma como se recogen y tabulan las lecciones aprendidas.

En la USPEC, frente al Plan de Continuidad de TI, se desempeñarán los siguientes roles:

### 5.1.1 Líder del Proceso Gestión de Tecnologías de la Información

El jefe de la Oficina de Tecnología tiene a su cargo la coordinación del equipo de tecnología, tanto interno, como aquel que desarrolla funciones en tecnología y que pertenezca a un contratista. Esto con el fin de brindar a la entidad la gestión necesaria para recuperar el ambiente de producción a fin de restituirlo a su estado normal.

Es responsable de:

#### Antes:

1. Realizar análisis de riesgo al proceso
2. Establecer el grado de criticidad del proceso.
3. Evaluar el impacto que la indisponibilidad de los servicios críticos de la entidad.
4. Estimar los tiempos de recuperación de los sistemas de información que soportan el proceso.
5. Determinar en qué punto del tiempo se deben retomar los datos de las aplicaciones (es decir, qué tanta información se puede perder sin afectar significativamente la actividad de la entidad).
6. Adelantar las gestiones necesarias para que los servicios tecnológicos puedan recuperarse después de un fallo Alto con las mismas características de calidad y desempeño que se tenían antes del incidente.
7. Proponer y facilitar la realización de pruebas de recuperación con su respectiva información.
8. Designar las funciones que sus colaboradores deban desarrollar antes y después de un desastre.
9. Canalizar ante la Dirección los proyectos y gastos relacionados con el mantenimiento y preparación de la plataforma tecnológica de la entidad.
10. Coordinar la ejecución de las pruebas de recuperación y actualizar el soporte de los procesos.
11. Implementar los planes de recuperación de desastres tecnológicos.

#### Durante:

1. Identificar causas de la indisponibilidad de los servicios.
2. Identificar los servicios afectados.

#### Después:

1. Verificar el adecuado funcionamiento de la plataforma.
2. Coordinar el retorno a normalidad.
3. Presentar a la Dirección el reporte sobre la recuperación de operaciones.
4. Verificar que el ambiente de contingencia, en caso de que aplique, continúa operando según lo establecido y que la protección permanece.

## 6. Premisas del plan de continuidad de TI

Al momento de la publicación del presente documento, la Oficina de Tecnología ha determinado evaluar la estrategia de contingencia para los siguientes servicios tecnológicos Directorio Activo, DNS y DHCP, Switch de Core y canales de internet desde el Centro de Cómputo de la entidad.
De igual forma, se establece que los lineamientos del presente plan se encuentran basados en las siguientes premisas:

- Los snapshot sobre las máquinas virtuales de la USPEC solo se realizan cuando se solicitan al administrador, por ende, no son programados.
- Las copias de respaldo se realizan cada 24 horas, pero se cuenta con historial de copias de más de 1 mes.
- No se cuenta con una estructura de contingencia para el chasis de Blades.
- Existe una redundancia de canales de internet con el mismo proveedor.
- Los equipos de usuarios finales, así como los servidores, cuentan con seguros contra daños, los cuales permiten solicitar nuevos equipos en caso de que estos sufran fallas irreversibles.
- Los sistemas, bases de datos, servicios y aplicativos web se encuentran respaldados por el backup de los proveedores de los servicios en la nube.

## 7. Centro de Cómputo

La Oficina de Tecnología ha establecido que su esquema de recuperación de los servicios críticos tecnológicos se realizará en el mismo centro de cómputo de la Entidad y la estrategia se enfoca en la recuperación vía copias de respaldo e instalación manual de los equipos.

Es responsabilidad de la Jefatura de la Oficina de Tecnología gestionar el mantenimiento a la plataforma tecnológica dispuesta en el Centro de Cómputo, así como las actualizaciones, reconfiguraciones o renovación que sean necesarias para mantener un servicio estable y seguro, para lo cual se seguirá lo establecido en el Plan de Mantenimiento desarrollado por la OTEC.

Cuando exista activos que presenten fallo o cuando se requiera actualización, tal necesidad se comunicará de manera inmediata por parte de los encargados de los mismos al Jefe de la Oficina de Tecnología quien autorizará los proyectos necesarios o elevará requerimiento a la Dirección General para que sean aprobados.

## 8. Aplicaciones críticas

Resultado de aplicar un análisis de los procesos de la entidad, se concluye que se requiere un Plan de Continuidad para los equipos que soportan los servicios priorizados de tecnología. Lo anterior con base en los valores definidos en la tabla de “Retorno a la normalidad” que permite determinar los tiempos de recuperación y de restauración para los servicios críticos de la entidad.

De acuerdo con lo anterior, la Oficina de Tecnología se enfocará en la recuperación de los siguientes servicios:

- Almacenamiento

- Base de datos
- Control de acceso físico
- DHCP
- DNS
- Clientes livianos
- Equipos servidores
- Impresión, copia y digitalización
- Internet
- Monitoreo y Seguridad
- Controlador de Dominio (AD)
- Telefonía
- Red (Cableada, Inalámbrica)
- Aplicaciones
  - Consecutivos
  - Intranet
  - Aplicativo de Inventarios
  - HELPTIC
  - MIPGestión
  - SEPEC
  - MAGICINFO
  - Turnos Facturas
  - Turnos Contratos

## 9. Tiempos y Momentos de recuperación

La Entidad ha establecido que los tiempos y momentos para la recuperación de los servicios (RTO y RPO) materia del alcance, deben ser iguales o inferiores a lo desplegado en la siguiente tabla:

**Nota:** La USPEC contempla los tiempos como deseables para proporcionar los servicios de manera óptima. Sin embargo, si no se cuenta con la estrategia de recuperación implementada, entonces el RTO se alinea con los valores definidos en la tabla de "Retorno a la normalidad".
Los servicios críticos son catalogados como aquellos que tienen la clasificación del impacto en niveles Alto y Medio
Una vez se realice la recuperación de los servicios críticos/priorizados, se debe iniciar con la recuperación de los servicios no críticos, los cuales están clasificados con nivel de Impacto "Bajo"

| Proceso | Servicio | Descripción del servicio | RTO | RPO | Impacto |
|---|---|---|---|---|---|
| Todos | Almacenamiento | Servidores y soluciones para centralizar el almacenamiento de la información de la entidad y de los usuarios | Entre 1 y 4 Horas | Entre 1 y 4 Hora | Alto |
| Todos | Backup | Servicios de backup y restauración de archivos de la entidad | Entre 1 y 4 Horas | Entre 1 y 8 Horas | Bajo |
| Todos | Base de datos | Sistemas de base de datos transversal a diferentes | Entre 1 y 4 Horas | Entre 0 y 1 Hora | Alto |

| | | | | | |
|---|---|---|---|---|---|
| | | aplicaciones de la entidad. Almacenamiento y control de datos de las aplicaciones. | | | |
| Gestión de las Tecnologías de la Información | Control de acceso físico | Servicio de control de acceso biométrico al centro de cómputo. | Entre 1 y 2 Días | Entre 1 y 2 Días | Bajo |
| Todos | DHCP | Servicio de asignación de IP dependiendo de la red donde esté el equipo. | Entre 1 y 2 Hora | Entre 4 y 8 Horas | Alto |
| Todos | DNS | El Domain Name System (DNS) es un servicio que habilita un enlace entre nombres de dominio y direcciones IP con la que están asociados | Entre 1 y 2 Hora | Entre 4 y 8 Horas | Alto |
| Todos | Clientes livianos | Equipo físico que se le asigna al usuario para el desarrollo de sus tareas. | Entre 1 y 2 Horas | 0 | Bajo |
| Todos | Equipos servidores | Equipos donde se soporta la plataforma tecnológica de la Entidad | Entre 1 y 2 Días | Entre 1 y 8 Horas | Alto |
| Todos | HELPTIC | Aplicación de Mesa de Ayuda y/o registros incidentes | Entre 1 y 4 Horas | Entre 4 y 8 Horas | Bajo |
| Todos | Impresión, copia y digitalización | Servicio de impresión, fotocopias y scanner de la entidad. | Entre 1 y 2 Hora | 0 | Medio |
| Todos | Internet | Servicio de conexión a Internet | Entre 0 y 1 Hora | 0 | Alto |
| Todos | Intranet | Sitio de información institucional para los funcionarios de USPEC. | Entre 8 y 24 Horas | Entre 8 y 24 Horas | Bajo |
| Gestión Administrativa y Financiera | Inventarios | Aplicativo de gestión y control de inventarios de la entidad. | Entre 8 y 24 Horas | Entre 8 y 24 Horas | Bajo |
| Gestión de las Tecnologías de la Información | Monitoreo | Equipos de monitoreo de seguridad y correlación de eventos. AlienVault. | Entre 1 y 4 Horas | Entre 0 y 1 Hora | Bajo |
| Todos | Seguridad de red | Equipos de seguridad para la red. Firewall, antivirus, entre otros. | Entre 0 y 1 Hora | Entre 4 y 8 Horas | Medio |
| Todos | Controlador de Dominio (AD) | Servicios de autenticación nombres de usuario, contraseñas que permiten a los usuarios autenticarse en el dominio de la entidad. | Entre 1 y 4 Hora | Entre 4 y 8 Horas | Alto |
| Todos | Servicios de red cableada | Servicios de red y cableado estructurado Conectividad de los equipos de la entidad a la red. | Entre 1 y 8 Horas | 0 | Alto |
| Todos | Servicios de red Inalámbrica | Servicios de conexión a la red de la entidad mediante la red inalámbrica. | Entre 0 y 2 Días | 0 | Alto |
| Gestión Estratégica | MIPGestion | Sistema Integrado de Gestión | Entre 8 y 24 | Entre 8 y 24 | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| Organizacional | | Institucional (SIGI) | Horas | Horas | |
| Gestión Administrativa y Financiera / Gestión Contractual | Turnos Facturas<br><br>Turnos Contratos | Módulo de aplicativo usado por el área contractual, en éste se ingresan todos los contratos de la unidad los cuales se gestionan mediante la asignación de un número consecutivos<br><br>Módulo de aplicativo usado por el área tesorería, mediante éste se gestiona la facturación de los contratos de la unidad de acuerdo con un consecutivo. | Entre 4 y 8 Horas | Entre 4 y 8 Horas | Bajo |

## 10. Activos críticos relacionados con la recuperación de servicios críticos

Para soportar las aplicaciones y servicios citados en el numeral anterior, la USPEC debe recuperar los siguientes activos (de software, hardware o servicios) en el centro de Cómputo de acuerdo con el inventario de activos de la entidad:

### Servicios con Impacto "Alto":

| Servicio crítico | Nombre del activo | Descripción del Activo |
|---|---|---|
| Almacenamiento | Switch interconexión de SAN HP 3PAR | Dispositivo de red de interconexión de almacenamiento y blade |
| | MC-3PAR-HP | Management Console - HP 3PAR StorServ |
| | SP-3PAR-HP | Service Procesor - HP 3PAR StorServ |
| | SRVFILESERVER - Servidor de File Server | Servidor para centralizar el almacenamiento de la data de los usuarios |
| | SRVSQLGD01 | FileServer, información compartida DINFRA y PRENSA |
| Base de datos | Software y backup de SQL Server 2014 | Motor de base de datos INFODOC, SIIEC y SIG |
| | Software Backup de MySQL | Motor de base de datos intranet, sistema de administración de inventarios |

| | | |
|---|---|---|
| Internet | Servicio de Internet | Servicio de conexión a Internet con el fin de asegurar el acceso a los servicios externos |
| Equipos servidores | HP Blade System C7000 Enclosure G3 | Cajón para servidores tipo blade |
| | Servidores HP Proliant BL460c Gen9 | Servidores físicos adecuados en el blade |
| | Framework y Componentes de VMWare | Servidores de servicio para habilitar la plataforma virtual |
| | Sistema Operativo Host - VMWare | Sistema Operativo VMWare 5.5 |
| | Sistema Operativo Windows Server 2012 | Sistema Operativo para servidor File Server y Directorio Activo |
| | Horizont View Administrator | Aplicación para la administración de escritorios por usuario |
| | Vsphere Manager | Aplicación para la administración del hardware de escritorio virtuales |
| Servicios de red cableada e inalámbrica | Switch de Core Cisco 93180 (hay 2) | Dispositivo principal de red |
| | Switch de Piso Cisco de 3560-3650 (de 24 y 48) 14 en total | Dispositivo de acceso de usuarios a la red |
| | Switch DELL Power Connect | Dispositivo de interconexión del datacenter |
| | Router Canal de Internet | Proveedor de Internet |
| DHCP | Servicio DHCP | Protocolo cliente-servidor que proporciona automáticamente un host de protocolo Internet (IP) con su dirección IP |
| DNS | Servicio DNS | El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información de nombres de dominio en redes |
| Controlador de Dominio (AD) | Servidor Controlador de Dominio | Backup Domain Controller (BDC) |
| | Servidor Directorio Activo - Virtual | Servidor principal/primario controlador de dominio Principal Domain Controller (PDC) |
| Seguridad de Red | Firewall Fortinet | Appliance Físico Fortigate 601E y 201E |

### Servicios con Impacto "Medio"

| Servicio crítico | Nombre del activo | Descripción del Activo |
|---|---|---|
| Equipos de trabajo | Estaciones de Trabajo Cliente Liviano | Equipo compuestos por Cliente liviano y pantalla |
| | Estaciones de Trabajo Portátiles | Computadores portátiles |
| | Escritorios Virtuales (Windows 10 Pro x64) | Entorno Windows para usuario final |
| Impresión, copia y digitalización | Impresoras | Impresoras de las diferentes dependencias |
| Seguridad de red | Appliance Iboss | Protección contra APT's |
| | Antivirus | Antimalware - Cliente / Consola Administración |
| Telefonía | Servicio de Telefonía | Servicio de telefonía suministrado por un tercero |
| Servicios de red cableada e inalámbrica | Switch Troncal SIP | Proveedor UNE |
| | Router Cisco | Proveedor UNE |
| | Switch Centros de cableado | Proveedor FAMOC |

### Servicios con impacto "Bajo"

| Servicio crítico | Nombre del activo | Descripción del Activo |
|---|---|---|
| Monitoreo | ESXi Appliance USM Alient Vault | Hypervisor sobre el que se ejecuta el correlacionador de eventos |
| | Appliances Unified Security Management (USM) Alien Vault | Correlacionador de Eventos |
| Servicios de desarrollo de software | Software de Desarrollo (PHP/MySQL) | Herramientas para desarrollo web y motor de base de datos |

| | | |
|---|---|---|
| | Servidor Virtual - SRVDESARROLLO | Servidor de desarrollo de aplicaciones |
| SIGI | Servidor Virtual - SRVSIGI<br>Magic Info | Servidor de Sistema Integrado de Gestión Institucional (SIGI)<br>Aplicativo de gestión de publicaciones en pantalla Samsung |
| | Servidor SRVGEO / SRV BD<br>MIPGestión | MIPGestión<br>Business Process Manager |
| Intranet | Intranet | Sitio de información institucional para los funcionarios de USPEC. |
| Aplicaciones | Servidor Virtual - VMCENTOSSRVAPP<br><br>Turnos Facturas<br><br>Turnos Contratos | Servidor de aplicaciones, aplicaciones Turnos Facturas y Contratos.<br><br>Módulo de aplicativo usado por el área tesorería, mediante éste se gestiona la facturación de los contratos de la unidad de acuerdo con un consecutivo.<br><br>Módulo de aplicativo usado por el área contractual, en éste se ingresan todos los contratos de la unidad los cuales se gestionan mediante la asignación de un número consecutivos |
| Backup | Acronis | Software de Backup |
| GLPI | Servidor Virtual - VMSVRAPP<br><br>Solución HELPTIC | Servidor de Aplicaciones, BD Consecutivos, GLPI, Site DINFRA<br><br>Solución Mesa de Ayuda y/o registro de incidentes |
| Inventarios | Servidor virtual - SRVBD<br><br>Inventarios | Servidor de Inventarios<br><br>Aplicativo de gestión y control de inventarios de la entidad. |
| Correo Electrónico | Google Password Sync | Agente para sincronización de contraseñas del directorio activo con la plataforma de correo electrónico |

## 11. Activación del plan de recuperación

### a. Detección Evento / Incidente

1. Como resultado bien sea de alguna emergencia o en razón a la monitorización permanente que la Oficina de Tecnología tiene de la plataforma tecnológica, se detecta algún evento o incidente que amenace la continuidad de las operaciones sobre la plataforma de producción.

2. La Oficina de Tecnología evaluará la magnitud del evento, así como su impacto en la operación, con el fin de evaluar alternativas que permitan continuar con la operación.
3. Si definitivamente no hay posibilidad de prestar servicio de manera habitual, el jefe de la Oficina de Tecnología se comunicará con la Dirección General de la entidad (o su delegado) e informará la situación presentada y de la misma forma solicita permiso para activar el Plan de Continuidad de TI.
4. La dirección general evalúa el evento y autoriza o niega el ingreso a modo contingente y/o la recuperación de los servicios que aplique.
5. Al obtener la aprobación para ingresar a modo contingente, el jefe de la Oficina de Tecnología informa a su equipo de trabajo y proveedores necesarios a fin de que se preparen para iniciar con la recuperación de los servicios.
6. Posterior a la actividad de contingencia el jefe de la Oficina de Tecnología informa a su equipo interno para efectuar las actividades de recuperación tecnológica de los servicios críticos para retornar al estado normal de operación.
7. Una vez se hayan recuperado los servicios críticos, se realiza el restablecimiento de los demás servicios, lo anterior de acuerdo con la clasificación realizada por la Entidad.
8. La Oficina de Tecnología se encarga de documentar y notificar cuando ya se encuentran los servicios restablecidos y funcionales.
9. Notificar a los usuarios la normalización de los servicios.

#### b. Comunicaciones

##### i. Comunicación corporativa

En el evento de emergencias, la comunicación sobre el incidente y actividades a desarrollar mientras se resuelve la situación serán informadas a través del correo electrónico y mediante la página Web, en caso de que estos se encuentren activos. Sin embargo, si no se encuentra activo ningún servicio, entonces la comunicación deberá hacerse a través de la oficina de comunicaciones por mecanismos alternos.

##### ii. Equipos de trabajo

El líder del proceso de Gestión de las tecnologías de la información deberá conservar la relación de los funcionarios y contratistas a su cargo y que son clave en las actividades de recuperación. La información de contacto incluye: teléfono celular, correo electrónico personal, número telefónico fijo y responsabilidades de cada persona en la recuperación de desastres.

## 12. Actividades de recuperación

El personal de la OTEC realizará las labores necesarias para activar la recuperación de desastres de los servicios críticos de acuerdo con la siguiente estrategia de recuperación:

### 12.1 Estrategia de la recuperación

Para efectuar la recuperación de los servicios se deberá tener en cuenta la siguiente clasificación de los servicios y sus requisitos basados en sus dependencias:

#### a. Dispositivos activos de red

Al activar el DRP, se requiere como mínimo el establecimiento de los equipos de comunicación tales como Switch Core, Switches de borde, equipos de firewall y de salida a internet.

### b. Sistema de Virtualización

Como requisito se deben tener los medios de instalación de los sistemas operativos que están instalados en los servicios críticos. Así mismo, es requisito mínimo contar con la copia de seguridad de las configuraciones de sistema operativo de acuerdo con los RPOs definidos.

### c. Bases de datos y Aplicaciones

Al activar el DRP, se requieren modificaciones a nivel de configuración de bases de datos. Así mismo, es necesario efectuar la restauración de la base de datos de los sistemas de información, así como los medios de instalación del software de base de datos de estos aplicativos. En este caso, se deben mantener respaldadas tanto las configuraciones como los datos de la aplicación de acuerdo con el RPO definido para cada aplicación.


## 12.2 Orden de la recuperación y sus actividades

Para efectuar la recuperación de desastres, se deben realizar las actividades de acuerdo a la prioridad de los servicios con impacto Alto, Medio y Bajo. Para la USPEC, luego de evaluar los servicios críticos, su impacto, Capa de recuperación y RTO se tiene la siguiente estructura de recuperación:

### Capa de servicios de red

a. Se descartan los servicios y activos con valor de impacto “Bajo” Estos se clasifican como NO críticos. Se recuperan posterior a la estabilización de los servicios críticos.

### Actividades de recuperación:

- Restaurar la copia de seguridad de configuraciones
- Validar con el proveedor de los equipos que se encuentren en el datacenter y que no son propiedad de la USPEC la recuperación y correcto funcionamiento de los mismos.
- Verificar el correcto funcionamiento de los equipos propiedad de la USPEC.
- Verificar el acceso a internet.

- Verificar el servicio de telefonía, comunicación con el proveedor para solicitar el restablecimiento del servicio.

De acuerdo con lo anterior se deben recuperar los servicios de capa de “Red” en el siguiente orden:

| Capa de recuperación | Servicio critico | Nombre del activo | Descripción del Activo | Tipo | RTO | RPO | Impacto | Orden de recuperación |
|---|---|---|---|---|---|---|---|---|
| Red | Servicios de red cableada | Switch Core Cisco 93180 (hay 2) | Dispositivo principal de red | Hardware | 1-8 horas | 0-1 hora | Alto | 1 |
| Red | Servicios de red cableada | Router Cisco | Proveedor de internet | Hardware | 1-8 horas | 0-1 hora | Medio | 1 |
| Red | Servicios de red cableada | Switch de Piso | Dispositivo de acceso de usuarios a la red | Hardware | 1-8 horas | 0-1 hora | Medio | 2 |
| Red | Servicios de red cableada | Switch DELL Power Connect | Dispositivo de interconexión del datacenter | Hardware | 1-8 horas | 0-1 hora | Medio | 2 |
| Red | Servicios de red cableada | Switch Huawei, Troncal SIP UNE | Proveedor UNE | Hardware | 1-8 horas | 0-1 hora | Medio | 2 |
| Red | Seguridad de red | Appliances Iboss | Protección contra APT's | Hardware | 1-8 horas | 4-8 horas | Medio | 3 |
| Red | Seguridad de red | Firewall Fortinet (FORTIUS PEC) | Appliance Físico Unified Threath Management (UTM) Fortigate 201E | Hardware | 1-8 horas | 4-8 horas | Alto | 3 |
| Red | DHCP | Servicio DHCP | Servicio automático de aprovisionamiento de direcciones IP | Servicios | 1-8 horas | 4-8 horas | Modera | 4 |
| Red | DNS | Servicio DNS | Servicio de resolución de nombres en la red | Servicios | 1-8 horas | 4-8 horas | Modera | 4 |
| Red | DNS | Simple DNS Plus | Software DNS Primario | Software | 1-8 horas | 4-8 horas | Bajo | 4 |
| Red | Internet | Canal de | Proveedor del | Servicios | 1-8 | 0-1 hora | Alto | 5 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Internet | Servicio de conexión a Internet | | horas | | | |
| Red | Telefonía | Planta Telefónica | Dispositivo para administración del servicio de telefonía en la sede principal | Hardware | 4-8 horas | 4-8 horas | Medio | 1 |
| Red | Telefonía | Teléfonos IP | Equipo de comunicación | Hardware | 4-8 horas | 4-8 horas | Medio | 2 |
| Red | Telefonía | Servicio de Telefonía | Servicio que la OTEC suministra a la USPEC | Servicios | 4-8 horas | 4-8 horas | Medio | 3 |

### Capa de virtualización

a. Se organizan los servicios por **"Capa de recuperación"** y se continúa con los servicios y sus activos de capa de **"Sistema Operativo".**

### Actividades de recuperación:

- Instalar y configurar el sistema de virtualización
- Instalar/restaurar las configuraciones del rol de controlador de dominio, DNS y DHCP interno.
- Instalar/restaurar las máquinas virtuales de los servicios de almacenamiento.
- Restauración y despliegue de máquinas virtuales. En caso de que no se cuente con backup de los snapshot, se deberán crear desde cero.
- Restaurar los backups de configuraciones de carpetas y permisos de acuerdo con las relaciones de confianza con los servidores de dominio.
- Verificar:
    - Conectividad con los servicios de red interna.
    - Navegación en internet
    - Asignación de direcciones DHCP
    - Resolución de nombres locales y en internet.
    - Requisitos adicionales como actualizaciones de software, aplicaciones complementarias de capa de sistema operativo.

- Restaurar las máquinas virtuales de HELPTIC y Servicios Web. En caso de que no se tenga backup de estas máquinas entonces deberán instalarse desde cero.
- Verificación de funcionamiento desde los equipos clientes.

De acuerdo con lo anterior se deben recuperar los servicios de capa de **"Virtualización"** en el siguiente orden:

| Capa de recuperación | Servicio Critico | Nombre del activo | Descripción del Activo | Tipo | RTO | RPO | Impacto | Orden |
|---|---|---|---|---|---|---|---|---|
| Virtualización | Equipos servidores | HP Blade System C7000 Enclosure G3 | Cajón para servidores tipo blade | Hardware | 4-48 horas | 0-1 hora | Medio | 1 |
| Virtualización | Almacenamiento | Switch interconexión de SAN HP 3PAR | Dispositivo de red de interconexión de almacenamiento y blade | Hardware | 1-8 horas | 0-1 hora | Alto | 1 |
| Virtualización | Equipos servidores | Servidores HP Proliant BL460c Gen9 | Servidores físicos adecuados en el blade | Hardware | 4-48 horas | 0-1 hora | Medio | 2 |
| Virtualización | Almacenamiento | SP-3PAR-HP | Service Procesor - HP 3PAR StorServ | Software | 1-8 horas | 0-1 hora | Alto | 2 |
| Virtualización | Equipos Servidores | Sistema Operativo Host - VMWare | Sistema Operativo VMWare 5.5 | Software | 4-48 horas | 0-1 hora | Medio | 3 |
| Virtualización | Equipos servidores | Framework y Componentes de VMWare | Servidores de servicio para habilitar la plataforma virtual | Software | 4-48 horas | 0-1 hora | Medio | 3 |
| Virtualización | Almacenamiento | MC-3PAR-HP | Management Console - HP 3PAR StorServ | Hardware | 1-8 horas | 0-1 hora | Alto | 3 |
| Virtualización | Equipos Servidores | Sistema Operativo Windows Server 2012 | Sistema Operativo para servidor File Server y Directorio Activo | Software | 4-48 horas | 0-1 hora | Medio | 4 |

| Capa de recuperación | Servicio Critico | Nombre del activo | Descripción del Activo | Tipo | RTO | RPO | Impacto | Orden |
|---|---|---|---|---|---|---|---|---|
| Virtualización | Almacenamiento | SRVFILESERVER - Servidor de File Server | Servidor para centralizar el almacenamiento de la data de los usuarios | Software | 1-8 horas | 0-1 hora | Alto | 4 |
| Virtualización | Almacenamiento | SRVSQLGD01 | FileServer, datas compartidas DINFRA y PRENSA | Software | 1-8 horas | 0-1 hora | Alto | 4 |
| Virtualización | Equipos servidores | Horizont View Administrator | Aplicación para la administración de escritorios por usuario | Software | 4-48 horas | 0-1 hora | Medio | 5 |
| Virtualización | Equipos servidores | Vsphere Manager | Aplicación para la administración del hardware de escritorio virtuales | Software | 4-48 horas | 0-1 hora | Medio | 5 |
| Virtualización | Equipos de trabajo | Escritorios Virtuales (Windows 10 Pro x64) | Entorno Windows para usuario final | Software | 1-4 horas | 1-2 días | Medio | 5 |
| Virtualización | Servicios de Autenticación y Controlador de Dominio (AD) | Servidores Directorio Activo - Virtual | Servidor principal/primario controlador de dominio Principal Domain Controller (PDC) | Software | 4-48 horas | 4-8 horas | Bajo | 6 |
| Virtualización | Equipos de trabajo | Estaciones de Trabajo (Cliente Liviano y portátiles) | Computadores de escritorio compuesta por caja cliente liviano y pantalla | Hardware | 1-4 horas | 1-2 días | Medio | 6 |
| Virtualización | Helptic | Servidor Virtual - VMSVRAPP | Servidor de Aplicaciones, BD Consecutivos, GLPI, Site DINFRA | Software | 1-4 horas | 4-8 horas | Bajo | 6 |

### Capa de Base de datos

a. Se organizan los servicios por "Capa de recuperación" y se continúa con los servicios y sus activos de capa de "Base de datos".

### Actividades de recuperación:

- Instalar/restaurar las máquinas virtuales de bases de datos
- Si no se cuenta con la copia de seguridad de las máquinas virtuales de bases de datos se debe instalar desde cero los productos MSSQL y MySQL.
- Restaurar las configuraciones o configurar manualmente bases de datos para puesta en operación.
- Restaurar los datos de las bases de datos.
- Validar la integridad de los datos restaurados.
- Preparar los enlaces entre base de datos y capas de aplicación.
- Verificar:
    - Conectividad con los servicios de red interna.
    - Navegación en internet (Si se requiere)
    - Asignación de direcciones DHCP
    - Resolución de nombres locales y en internet.
    - Comunicación con servicios dependientes.
    - Acceso, consultas y lecturas de datos dentro de las bases de datos.
    - Requisitos adicionales como actualizaciones de software, aplicaciones complementarias de capa de base de datos.

De acuerdo con lo anterior se deben recuperar los servicios de capa de "Base de datos" en el siguiente orden:

| Capa de recuperación | Servicio critico | Nombre del activo | Descripción del Activo | Tipo | RTO | RPO | Impacto | Orden |
|---|---|---|---|---|---|---|---|---|
| Base de datos | Base de datos | SQL Server 2014 | Construplan, SIIEC y SIG | Software | 1-4 horas | 0-1 hora | Alto | 1 |
| Base de datos | Base de datos | MySQL | Motor de base de datos intranet, sistema de administración de inventarios | Software | 1-4 horas | 0-1 hora | Alto | 2 |

## II. Capa de Aplicaciones

a. Se organizan los servicios por "**Capa de recuperación"** y se continúa con los servicios y sus activos de capa de **"Aplicaciones".**

### Actividades de recuperación:

- Dado que en este punto el servicio de internet ya debe encontrarse recuperado se debe realizar la verificación de las aplicaciones externas que son utilizadas por internet:
    - Correo electrónico, SUIFP, SPI, FURAG, SIGEP, Software de Nomina Humano (Cloud)
- Dado que en este punto el servicio de virtualización ya debe encontrarse recuperado se debe realizar la verificación de las aplicaciones internas (Infodoc, consecutivos, Helptic, SEPEC, etc.)

- Configurar los parámetros de integración entre bases de datos y aplicaciones.
- Realizar pruebas integradas de aplicación y de base de datos generales. En este caso se deberá trabajar en conjunto para resolver cualquier problema que se presente con la aplicación.
- Validar la integridad de los datos presentados en la aplicación.

De acuerdo con lo anterior se deben recuperar los servicios de capa de “Aplicación” en el siguiente orden:

| Capa de recuperación | Servicio critico | Nombre del activo | Descripción del Activo | Tipo | RTO | RPO | Impacto | Orden |
|---|---|---|---|---|---|---|---|---|
| Aplicaciones | Impresión, copia y digitalización | Impresora HP | Impresoras marca HP instaladas en las diferentes dependencias | Hardware | 0-1 hora | 1-2 días | Medio | 5 |
| Aplicaciones | GLPI | Solución HELPTIC | Solución Mesa de Ayuda y/o registro de incidentes | Software | 1-4 horas | 4-8 horas | Bajo | 2 |
| Aplicaciones | Monitoreo | Appliances Unified Security Management (USM) Alien Vault | Correlacionador de Eventos | Software | 1-4 horas | 0-1 hora | Bajo | 4 |
| Aplicaciones | Servicios de desarrollo de software | Software de Desarrollo (PHP/MySQL) | Herramientas para desarrollo web y motor de base de datos | Software | 4-8 horas | 8-24 horas | Bajo | 2 |
| Aplicaciones | Turnos Facturas / Turnos Contratos | Turnos Contratos Turnos facturas | Módulo de aplicativo usado por el área contractual y financiera, en éste se ingresan todos los contratos de la unidad los cuales se gestionan mediante la asignación de un número consecutivos | Software | 4-8 horas | 4-8 horas | Bajo | 3 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Aplicaciones | Seguridad de red | Antivirus Kaspersky | Antimalware - Consola Administración | Software | 4-8 horas | 4-8 horas | Medio | 6 |
| Aplicaciones | Seguridad de red | Antivirus Kaspersky | Antimalware - Cliente | Software | 4-8 horas | 4-8 horas | Medio | 7 |
| Aplicaciones | Servicios de Autenticación y Controlador de Dominio (AD) | Google Password Sync | Agente para sincronización de contraseñas del directorio activo con la plataforma de correo electrónico | Software | 4-8 horas | 4-8 horas | Bajo | 8 |
| Aplicaciones | SIGI | Servidor Virtual - SRVSIGI | Servidor de Sistema Integrado de Gestión Institucional (SIGI) | Software | 8-24 horas | 8-24 horas | Bajo | 1 |
| Aplicaciones | SIGI | MIPGESTION | Business Process Manager | Software | 8-24 horas | 8-24 horas | Bajo | 3 |
| Aplicaciones | SIGI | Magic Info | Aplicativo de gestión de publicaciones en pantalla Samsung | Software | 8-24 horas | 8-24 horas | Bajo | 4 |
| Aplicaciones | Inventarios | Inventarios | Aplicativo de gestión y control de inventarios de la entidad. | Software | 8-24 horas | 8-24 horas | Bajo | 5 |
| Aplicaciones | Intranet | Intranet | Sitio de información institucional para los funcionarios de USPEC. | Software | 8-24 horas | 8-24 horas | Bajo | 6 |

### 12.3 Retorno a Normalidad

Por considerarse una recuperación vía backups y manual, la recuperación en si constituye el mismo ambiente de producción, por tanto, no hay actividades adicionales.
El jefe de la Oficina de Tecnología se comunica con la Dirección (o alguno de los delegados) e informa la disponibilidad de los servicios y efectividad del DRP.
A continuación, se presenta la tabla con los valores de tiempo que requiere el área de tecnología para efectuar el retorno a la normalidad para cada uno de los servicios críticos.

**Nota:** Dado que los RTOs varían o son inferiores al tiempo de retorno a la normalidad, entonces la entidad deberá establecer estrategias de contingencias adecuadas para varios de los servicios.

| Servicio Crítico | Descripción | Tiempo de recuperación | RTO | Nota |
|---|---|---|---|---|
| Almacenamiento | Servidores y soluciones para centralizar el almacenamiento de la información de la entidad y de los usuarios | 8 horas | Entre 1 y 8 Horas | Se cuenta con servicio de Backup |
| Backup | Servicios de backup y restauración de archivos de la entidad | 4 horas | Entre 8 y 24 Horas | Dentro del tiempo de recuperación |
| Base de datos | Sistemas de base de datos transversal a diferentes aplicaciones de la entidad. Almacenamiento y control de datos de las aplicaciones. | 1 hora | Entre 0 y 1 Hora | Dentro del tiempo de recuperación |
| Control de acceso físico | Servicio de control de acceso biométrico al centro de cómputo. | 8 horas | Entre 1 y 2 Días | Dentro del tiempo de recuperación |
| Sincronización Correo electrónico | Servicio de Correo Electrónico Google Gsuite de USPEC, Administrado por la OTEC. Sincronización con el directorio activo, | 4 horas | Entre 8 y 24 Horas | Dentro del tiempo de recuperación |
| DHCP | Protocolo cliente-servidor que proporciona automáticamente un host de protocolo Internet (IP) con su dirección IP | 4 horas | Entre 0 y 1 Hora | Contingencia existente |
| DNS | El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet | 4 horas | Entre 0 y 1 Hora | Contingencia existente |
| Equipos de trabajo | Servicio de aprovisionamiento, mantenimiento y soporte de los equipos estaciones de trabajo. | 24 horas | Entre 1 y 4 Horas | Trabajo Remoto |
| Equipos servidores | Servicio de servidores y equipos transversales para soportar las aplicaciones de la entidad. | 24 horas | Entre 0 y 1 Hora | Se realizan snapshot a las MV de las app de la entidad las |

| | | | | |
|---|---|---|---|---|
| | | | | cuales se realizan los martes y viernes |
| HELPTIC | Solución Mesa de Ayuda y/o registro de incidentes | 8 horas | Entre 1 y 4 Horas | "Correo" |
| Impresión, copia y digitalización | Servicio de impresión, fotocopias y scanner de la entidad. | 8 horas | Entre 0 y 1 Hora | Servicio externo - ANS |
| Internet | Servicio de conexión a Internet | 4 horas | Entre 0 y 1 Hora | Contingencia Existente |
| Intranet | Sitio de información institucional para los funcionarios de USPEC. | 8 horas | Entre 8 y 24 Horas | Dentro del tiempo de recuperación |
| Inventarios | Aplicativo de gestión y control de inventarios de la entidad. | 8 horas | Entre 8 y 24 Horas | Dentro del tiempo de recuperación Contingencia Existente |
| Monitoreo | Equipos de monitoreo de seguridad y correlación de eventos. AlienVault | 24 horas | Entre 1 y 4 Horas | No cuenta con contingencia |
| Seguridad de red | Equipos de seguridad para la red. Firewall, antivirus, entre otros. | 8 horas | Entre 0 y 1 Hora | Firewall: Este equipo cuenta con sistema de alta disponibilidad (HA) |
| Controlador de Dominio (AD) | Servicios de autenticación nombres de usuario, contraseñas que permiten a los usuarios autenticarse en el dominio de la entidad. | 8 horas | Entre 0 y 1 Hora | Contingencia (PrimaryDomain Controler-BackupDomainController) |
| Servicios de desarrollo de software | Servicios relacionados con el desarrollo de componentes y casos de uso en diferentes aplicaciones de la entidad. | 2 horas | Entre 4 y 8 Horas | Dentro del tiempo de recuperación |
| Servicios de red cableada | Servicios de red y cableado estructurado Conectividad de los equipos de la entidad a la red. | 2 horas | Entre 0 y 1 Hora | "Se cuenta con Switch de respaldo" |
| Servicios de red Inalámbrica | Servicios de conexión a la red de la entidad mediante la red inalámbrica. | 2 horas | Entre 8 y 24 Horas | Dentro del tiempo de recuperación |
| MIPGESTION | Sistema Integrado de Gestión Institucional (SIGI) | 24 horas | Entre 8 y 24 Horas | Dentro del tiempo de recuperación |
| Telefonía | Servicio que la OTEC suministra a la USPEC | 8 horas | Entre 4 y 8 Horas | Dentro del tiempo de recuperación |

| | | | | |
|---|---|---|---|---|
| Turnos Facturas / Turnos Contratos | Módulo de aplicativo usado por el área contractual, en éste se ingresan todos los contratos de la unidad los cuales se gestionan mediante la asignación de un número consecutivos<br><br>Modulo de aplicativo usado por el área tesorería, mediante éste se gestiona la facturación de los contratos de la unidad de acuerdo con un consecutivo. | 8 horas | Entre 4 y 8 Horas | Dentro del tiempo de recuperación |

## 13. Contingencias actuales

A la fecha de elaboración del presente plan se cuentan con las siguientes contingencias para algunos de los servicios. Sin embargo, para los servicios que no se mencionen a continuación deberán definirse las contingencias respectivas como parte del Plan de Continuidad de Negocio.

| Código | Proceso | Servicio Crítico | Nombre del Procedimiento | Descripción del Procedimiento | ¿Tiempo de operación bajo el procedimiento o manual? | ¿Está documentado? |
|---|---|---|---|---|---|---|
| A3 | Gestión de las Tecnologías de la Información | Virtualización | Restablecimiento servicio de máquinas virtuales | Snapshot en los almacenamientos | 8 horas | Si |
| A3 | Gestión de las Tecnologías de la Información | Backup | Backup Manual | Se realizan las copias de los archivos en la unidad de almacenamiento de la entidad. | 8 horas | Si |
| A3 | Gestión de las Tecnologías de la Información | Seguridad de Red | Configuración de Internet Manual | Se realiza una configuración para la salida a internet de los usuarios sin restricciones | 8 horas | Si |
| A3 | Gestión de las Tecnologías de la Información | DHCP | Habilitar el servicio de DHCP en otra maquina | Habilitar el servicio de DHCP en otra maquina | 8 horas | Si |

| | | | | | | |
|---|---|---|---|---|---|---|
| A3 | Gestión de las Tecnologías de la Información | Estaciones de trabajo | Acceso por VPN | En caso de que se generen daños en los equipos, se notifica el evento a la compañía aseguradora para que se autorice la reposición de los equipos.<br><br>Los usuarios acceden a los escritorios virtuales a través de VPN | 24 horas | Si |
| A3 | Gestión de las Tecnologías de la Información | Internet | Canal redundante | Se cuenta con un canal de internet redundante. En caso de que se afecte el servicio en el canal principal, entra en operación automática el backup. | 8 horas | No requiere, servicio automatizado |
| A3 | Gestión de las Tecnologías de la Información | Controlador de Dominio (AD) | Controlador de dominio alterno | Se encuentra en contingencia con el servidor del Backup del controlador de dominio | 8 horas | Si |
| A3 | Gestión de las Tecnologías de la Información | Intranet | Envío de desprendibles de Nomina | Se envía el enlace para el acceso al comprobante de pago de nómina por correo electrónico. | 8 horas | Si “Guía Humano” |

## 14. Riesgos frente a la recuperación de desastres (DRP)

A continuación, se listan los riesgos identificados al momento de implementar el plan de Recuperación de Desastres (DRP). Como resultado de esto deben implementarse acciones de tratamiento de estos con el fin de mitigar el riesgo.

| RIESGO | PROCESO/ ÁREA | CAUSA DEL RIESGO | CONSECUENCIAS POTENCIALES | CONTROLES EXISTENTES | Riesgo Inicial (teniendo en cuenta los controles actuales) | | | MEDIDA DE TRATAMIENTO DEL RIESGO | ACCIONES DEL PLAN DE TRATAMIENTO |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | PROB (1-5) | IMP (1-5) | RIESGO (P*I) | | |
| Fuga de información de los procesos de la entidad | Oficina de Tecnología | 1. Exposición directa de la información durante la etapa de recuperación o en la contingencia.<br><br>2. Ataques informáticos, Instalación de virus, o programa maligno en equipos portátiles que usen los funcionarios o contratistas durante la recuperación o contingencia.<br><br>3. Extracción de información de los equipos que serán reemplazados y que no han sido cifrados.<br><br>4. Abuso de los contratistas o terceros que tengan contacto con la información. | 1. Multas y acciones legales a la entidad.<br><br>2. Perdida de confiabilidad por parte de las entidades y usuarios que consumen los servicios externos de la Entidad. | 1. Segregación de funciones en la recuperación de los servicios, así como roles y responsabilidades en la dirección del DRP.<br><br>2. Proceso de gestión de cambios, donde se describen las actividades que requieren aprobación y rollback con el fin de mitigar riesgos de afectación de servicios.<br><br>3. Supervisión de los contratistas o terceros que tenga acceso a los sistemas de información. | 2 | 4 | Alto | Reducir | 1. Realizar pruebas reales de la recuperación de desastres para verificar las actividades y los escenarios con claridad donde podría materializarse el riesgo.<br><br>2. Durante la recuperación, debe utilizarse software debidamente descargado de otras fuentes que no expongan a internet la información de la entidad.<br><br>3. Garantizar que los equipos implementan cifrado de disco duro, cifrado de datos en las bases de datos y en los backups. |
| Modificación no autorizada o accidental de la información de la entidad | Oficina de Tecnología | 1. Planeación inadecuada de la recuperación de desastres.<br><br>2. Sobrescritura de la | 1. Perdida de disponibilidad de los servicios proporcionados a los usuarios internos. | 1. Definición del plan de recuperación de desastres, planes y orden de recuperación.<br><br>2. Proceso de | 2 | 4 | Alto | Reducir | 1. Planear los escenarios de recuperación, listando todos los componentes necesarios para una recuperación completa. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | información más vigente con información antigua.<br><br>3. Desconocimiento de los nombres de archivos, repositorios, tipos de configuración que se van a recuperar. | 2. Retraso en actividades misionales de la entidad por causa de falta de acceso a los recursos.<br><br>3. Datos inexactos y sin calidad.<br><br>4. Reprocesos en la generación de la información.<br><br>5. Incumplimientos legales por publicación de información inexacta. | gestión de cambios, donde se describen las actividades que requieren aprobación y rollback con el fin de mitigar riesgos de afectación de servicios.<br><br>3. Estructuración y preparación de las formas de recuperación, así como pruebas de recuperación periódicas. | | | | | 2. Socializar los roles y el orden de la recuperación de los sistemas críticos a cada uno de los involucrados.<br>3. Estructurar pruebas en ambiente de laboratorio, previos de implementación del plan en la Entidad.<br>4. Documentar la información de pasos y configuraciones para la recuperación de los servicios. |
| Retrasos en la recuperación frente al tiempo de recuperación planteado. | Oficina de Tecnología | 1. Pérdida de la información que se está recuperando porque no se encuentran los backups.<br><br>2. Los backups no sirven o no están íntegros.<br>3. La copia de seguridad se recupera y no contiene la información de la fecha esperada.<br>4. No se cuenta con backups de algunas aplicaciones y deben hacerse manuales.<br>5. Las aplicaciones no se integran como se esperaba inicialmente.<br>6. Equipos o servicios sin contingencia | 1. Denegación de los servicios prestados por la entidad<br><br>2. Sanciones, incumplimiento de requisitos legales. | 1. Proceso de gestión de cambios, donde se describen las actividades que requieren aprobación y rollback con el fin de mitigar riesgos de afectación de servicios.<br><br>2. Verificación de integridad y seguridad de los backups.<br><br>3. Pruebas de restauración periódicas. | 1 | 4 | Alto | Reducir | 1. Realizar pruebas reales de la recuperación de desastres para verificar las actividades y los escenarios con claridad donde podría materializarse el riesgo.<br><br>2. Implementar solución de respaldo de archivos en tiempo real, que se guarde una réplica de los archivos en otro servidor. |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | s<br>7. Las pruebas de los servicios no funcionan y debe solicitarse soporte. | | | | | | | |

## 15. Pruebas del DRP

El plan de Recuperación de desastres (DRP) debe ser probado al menos dos (2) veces al año. Es responsabilidad del líder del proceso gestionar la realización de una prueba anual en la que se verifique la operación de los procesos y componentes contingentes. Las pruebas se deben programar al menos con dos meses de antelación.
Los tipos de pruebas que se pueden realizar son:

**Pruebas Unitarias**
Se prueba cada elemento que compone la solución de respaldo en forma independiente. No se afectan los servicios de producción. Aquí se deben realizar pruebas de backup y restauración de configuraciones por cada elemento (sistema operativo, aplicación, datos) critico.

**Pruebas integradas**
Se prueban en forma integrada dos o más componentes de la solución de respaldo sin afectar los servicios de producción. Aquí se realizan pruebas de las soluciones completas, varios servidores, con su aplicación y su base de datos. Por ejemplo, para el caso del directorio activo, las pruebas incluyen los 3 servicios: Directorio Activo, DNS y DHCP.

**Pruebas totales**
Verifican el funcionamiento de todos los elementos descritos en el Plan de Recuperación de Desastres. En esta prueba se simula una caída y recuperación total de los servicios actuales. Se realizan las mediciones correspondientes y se actualiza el plan de recuperación de desastres. Sin embargo, para que esta prueba sea exitosa y no se afecte de forma negativa la entidad, debe estar acompañada por las estrategias de contingencia del Plan de Continuidad de Negocio.

**Revisó**: Camilo Alejandro Romero González
Coordinador Grupo de Comunicaciones

**Elaboró:** Ricardo Díaz Rodríguez
Profesional Universitario
Álvaro Camargo Barbosa
Analista de Sistemas
Fernando Vargas Herrera
Técnico Operativo