***PLAN DE RECUPERACIÓN ANTE DESASTRES “DRP”, DEL (NOMBRE DEL SISTEMA DE INFORMACIÓN QUE CORRESPONDA)***

|  |
| --- |
| **HISTÓRICO DE REVISIONES.** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha** | **Versión** | **Descripción** | **Autores** |
| *AAAA/MM/DD* |  | *(Describa los cambios incorporados en la versión, si es la primera, escriba: Documento Inicial)* | *(Nombres de los colaboradores que construyeron el contenido de este registro)* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **CONTENIDO** |

[**1.** **DESCRIPCIÓN DEL DOCUMENTO** 4](#_Toc185432795)

[1.1 Propósito 4](#_Toc185432796)

[1.2 Generalidades 4](#_Toc185432797)

[1.3 Referencias Normativas 4](#_Toc185432798)

[1.4 Glosario 5](#_Toc185432799)

[**2.** **INTRODUCCIÓN** 7](#_Toc185432800)

[2.1 A Quién va dirigido el manual 7](#_Toc185432801)

[2.2 Organización del Manual 7](#_Toc185432802)

[**3.** **OBJETIVO** 7](#_Toc185432803)

[**4.** **ANTECEDENTES** 7](#_Toc185432804)

[**5.** **GENERALIDADES - DRP DEL *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** 8](#_Toc185432805)

[5.1 Descripción del DRP 8](#_Toc185432806)

[5.2 Entorno del *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN* 9](#_Toc185432807)

[5.3 Alcance del DRP 9](#_Toc185432808)

[**6.** **INCIDENTES GRAVES DE CONTINUIDAD DEL *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** 9](#_Toc185432809)

[6.1 Actividades de prevención 10](#_Toc185432810)

[6.2 Equipo de Recuperación DRP del *abreviatura/nombre del sistema de información* 10](#_Toc185432811)

[6.2.1 Grupo Responsable de la Gestión de Crisis 11](#_Toc185432812)

[6.2.2 Roles y Responsabilidades 11](#_Toc185432813)

[6.3 Activación y Notificación DRP 14](#_Toc185432814)

[6.3.1 Activación DRP 14](#_Toc185432815)

[6.3.2 Notificación DRP 14](#_Toc185432816)

[**7.** **PLATAFORMA TECNOLÓGICA DEL *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** 17](#_Toc185432817)

[7.1 Infraestructura Crítica del *abreviatura/nombre del sistema de información* 17](#_Toc185432818)

[7.2 Servidores del *abreviatura/nombre del sistema de información* 17](#_Toc185432819)

[7.3 Arquitectura del *abreviatura/nombre del sistema de información* - IFX 18](#_Toc185432820)

[7.4 Arquitectura Bochica 18](#_Toc185432821)

[7.5 Caracterización Servidores del *abreviatura/nombre del sistema de información* 18](#_Toc185432822)

[7.6 Arquitectura de Aplicaciones y Servicios del *abreviatura/nombre del sistema de información* 18](#_Toc185432823)

[**8.** **ACTIVIDADES DE GESTIÓN DE CRISIS** 19](#_Toc185432824)

[**9.** **MANTENIMIENTO DEL DRP *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** 20](#_Toc185432825)

[9.1 Actualización manual DRP *abreviatura/nombre del sistema de información* 20](#_Toc185432826)

[**10.** **PLAN DE PRUEBAS *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** 21](#_Toc185432827)

[10.1 Tabla de Errores 21](#_Toc185432828)

[10.2 Contingencia y Soporte 21](#_Toc185432829)

[10.2.1 Encendido del *abreviatura/nombre del sistema de información* en el Data Center Alterno (Bochica) *(Este punto es solo si aplica)* 21](#_Toc185432830)

[10.3 Plan de Pruebas 22](#_Toc185432831)

[**11.** **GLOSARIO DE TÉRMINOS** 23](#_Toc185432832)

[**12.** **ANEXOS** 23](#_Toc185432833)

[12.1 Matriz de Escalamiento 23](#_Toc185432834)

|  |
| --- |
| 1. **DESCRIPCIÓN DEL DOCUMENTO** |

|  |
| --- |
| Propósito |

Este documento tiene el propósito de facilitar la toma de decisiones ante una emergencia que se presente con el *Nombre del sistema de información*, en adelante *abreviatura si aplica*, de la Superintendencia de Industria y Comercio.

|  |
| --- |
| Generalidades |

La recuperación ante desastres se ha definido tradicionalmente como la recuperación de los sistemas de TI después de eventos de interrupción que causan fallas en los sistemas, tales como vandalismo, huracanes e inundaciones que tiene como resultado la falta de acceso o interrupciones prolongadas de energía y comunicación. La recuperación del negocio se define como el restablecimiento de todos los procesos de misionales críticos que son necesarios para continuar o restablecer las operaciones. La recuperación incluye: la recuperación ante desastres, gestión de crisis, gestión de emergencias y plan de comunicaciones.

El Plan de Recuperación ante Desastres del *abreviatura o nombre del sistema de información* documenta las principales actividades que deben realizarse ante una interrupción prolongada del sistema y soporta las acciones y decisiones necesarias para restablecer el sistema a su nivel operativo en condiciones de normalidad.

|  |
| --- |
| Referencias Normativas |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Jerarquía de la norma** | **Numero/Fecha** | **Título** | **Artículo** | **Aplicación Específica** |
|
| Decreto Nacional | 1008 del 14 de junio de 2018 | Política de Gobierno Digital | Artículo 2.2.9.1.1.1 al 2.2.9.1.4.2 | Aplicación total |
| Norma Técnica Colombiana | ISO 27001 | Tecnología de Información, Técnicas de seguridad Sistemas de gestión de la seguridad de la información | Ítem A.17 | Aspectos de seguridad de la información, de la Gestión de Continuidad de Negocio. |
| Norma Técnica Colombiana | ISO 22301 | Seguridad y resiliencia. Sistema de gestión de continuidad de negocio. Requisitos | Aplicación total | Aplicación total |
| Norma Técnica Colombiana | ISO 27031 de 2016 | Tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de la información y las comunicaciones para la continuidad del negocio. | Aplicación total | Aplicación total |

|  |
| --- |
| Glosario |

ANÁLISIS DE IMPACTO AL NEGOCIO (BIA): Proceso en el que se analiza el impacto de una interrupción conforme avanza el tiempo.

CONTINUIDAD DE NEGOCIO: Capacidad de una organización de continuar la oferta de productos y servicios dentro de un período de tiempo aceptable a una capacidad predefinida durante una interrupción.

DESASTRE: Es un evento nocivo, inesperado o imprevisible, que afecta seriamente el funcionamiento normal de los trámites y servicios de TI.

LIF: Laboratorio de Informática Forense.

INTERRUPCIÓN: Incidente bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización.

MTPD: Periodo de tiempo dentro del cual el impacto de no reanudar las actividades sería inaceptable para la organización.

OPERACIÓN NORMAL: Es la operación de los trámites y servicios tal como funcionan actualmente, esto es, cada servicio es soportado en la sede en la que fue definida originalmente.

OPERACIÓN INTERRUMPIDA: Es el periodo de tiempo transcurrido entre el evento de un desastre que causa indisponibilidad de los servicios y la recuperación de la operación, ya sea en sitio principal o alterno.

OPERACIÓN ALTERNA: La operación Alterna se da en el momento que se activa el sitio de contingencia como soporte para la prestación de los servicios de TI; en la operación Alterna se debe tener en cuenta que la capacidad de los recursos podría no ser la misma de la operación normal, por lo cual algunos procesos podrían tomar más tiempo en su ejecución, o podría no haber capacidad de atención del 100% de la operación.

OPERACIÓN RESTABLECIDA: Este estado se alcanza cuando se ha retornado la operación de todos los servicios a su estado normal, esto es, todos los servicios y componentes de aplicación se encuentran ejecutando correctamente y bajo las mismas condiciones que presentaba antes del desastre.

PLAN DE CONTINUIDAD DE NEGOCIO: Información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio.

RPO: Corresponde al punto en el cual se retoma la información en caso de recuperación. Se asocia al último respaldo generado en las aplicaciones

RTO: Período de tiempo dentro del MTPD, para reanudar las actividades interrumpidas en una capacidad aceptable mínima especificada.

TRÁMITE: Conjunto de requisitos, pasos, o acciones reguladas por el Estado, dentro de un proceso misional, que deben efectuar los ciudadanos, usuarios o grupos de interés ante una Entidad u organismo de la administración pública o particular que ejerce funciones administrativas, para acceder a un derecho, ejercer una actividad o cumplir con una obligación, prevista o autorizada por la ley.

|  |
| --- |
| 1. **INTRODUCCIÓN** |

Se dispone de este manual operativo para facilitar el normal funcionamiento de los servicios del *abreviatura/nombre del sistema de información* y ante uno o más incidentes de desastre que afecten el sistema, optar por activar el DRP en un sistema alterno mediante estrategias de continuidad hasta llegar al restablecimiento del sistema a su condición de normalidad en el centro de datos principal.

|  |
| --- |
| A Quién va dirigido el manual |

El presente documento está dirigido a todos los funcionarios y contratistas de la Oficina de Tecnología e Informática y líderes de procesos misionales, de la Superintendencia de Industria y Comercio, en adelante SIC, que se encuentren relacionados con la continuidad de los servicios de TI y que están vinculados con la operación del *abreviatura/nombre del sistema de información*.

|  |
| --- |
| Organización del Manual |

Este manual dispone las estrategias necesarias que deben ser implementadas para la recuperación del *abreviatura/nombre del sistema de información*, a partir de unos factores que activaría el DRP, y la definición de los roles y responsabilidades para restablecer el sistema en un esquema de recuperación y luego en operación de normalidad.

|  |
| --- |
| 1. **OBJETIVO** |

Implementar las estrategias para apoyar la continuidad en la prestación de los servicios y trámites del *abreviatura/nombre del sistema de información* de la entidad, a través de la recuperación del sistema de información ante la materialización de escenarios de desastre que puedan causar la interrupción total o parcial del *abreviatura/nombre del sistema de información*.

|  |
| --- |
| 1. **ANTECEDENTES** |

Para el normal desarrollo de este plan se contempla lo siguiente:

* Se cuenta con un centro de cómputo que puede ser utilizado como centro alterno. Está ubicado en piso quinto de la sede Bochica y con la debida adecuación, contará con las características físicas y lógicas necesarias para soportar la infraestructura de TI para la contingencia.
* El personal requerido (coordinadores de equipos de trabajo, funcionarios, contratistas y especialistas) estarán disponibles durante el desastre.
* Los procedimientos de operación, manuales de usuario y diagramas de arquitectura de los sistemas de información de la Entidad deben estar documentados y actualizados.

|  |
| --- |
| 1. **GENERALIDADES - DRP DEL *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** |

La Superintendencia de Industria y Comercio requiere implementar su estrategia de recuperación ante desastres, para lo cual cuenta con los resultados del Análisis de Impacto al Negocio “BIA”, el cual presenta una lista priorizada de sistemas de información críticos. Además, tiene en su estrategia una hoja de ruta alineada con el Plan Estratégico de Tecnología de la Información en la cual se definió que en 2021 se implementará un sistema misional en esquema de recuperación de desastres.

|  |
| --- |
| Descripción del DRP |

El *abreviatura/nombre del sistema de información*, es el seleccionado por la SIC, para que sea implementado en la primera fase del DRP de la entidad. Debe permitir continuar con la prestación de *# de trámites y/o servicios* gestionados por *la delegatura/dependencia propietaria del sistema* de la SIC. Esta selección se puede explicar por *describa el contexto en el que se desarrolla el DRP, puede utilizar elementos desarrollados en otros instrumentos como el Análisis de Impacto al Negocio “BIA”.*

El *abreviatura/nombre del sistema de información* soporta tecnológicamente los *# de trámites y/o servicios en qué material*. El soporte es brindado por el proveedor *nombre del proveedor* quien *periodicidad con que* genera nuevas funcionalidades al aplicativo, tanto a nivel normativo como funcional. *(si aplica)*

Lo anterior, se detalla a continuación:

|  |
| --- |
| Entorno del *abreviatura/nombre del sistema de información* |

*Describa los requerimientos técnicos y de conectividad del sistema de información para operar correctamente dentro de su entorno. Específicamente, detalle las dependencias necesarias para que el sistema interactúe con otras plataformas y servicios, tanto internos como externos, incluyendo, integración con otros sistemas, dependencias externas, y servicios complementarios.*

|  |
| --- |
| Alcance del DRP |

Este “Plan de Recuperación ante Desastres”, cubre exclusivamente las estrategias de recuperación de la infraestructura tecnológica para la operación de los trámites y servicios del *abreviatura/nombre del sistema de información*, de acuerdo con la priorización en el Análisis de Impacto al Negocio -BIA.

|  |
| --- |
| 1. **INCIDENTES GRAVES DE CONTINUIDAD DEL *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** |

Los incidentes graves que requieren la activación del DRP del SIPI se pueden clasificar en dos tipos. Así:

Incidentes por daño físico:

* + Sistema inactivo e inaccesible por falla física en los servidores
  + Daño en el Data Center por accesos no autorizados (vandalismo, hurto, terrorismo, infiltración, extorsión, afectación premeditada, entre otros)
  + Daño en el canal de comunicación y/o en el canal internet
  + Daños físicos (Incidentes naturales por incendio, terremoto, inundación, entre otros)
  + Fallas eléctricas y/o generadores de incendios, cortes de fluido eléctrico prolongado

Incidentes por daño lógico o software malicioso:

* + Ciberataques - Incidente por vulneración de los servicios (DDOS, código malicioso, suplantación, ramsonware, accesos no autorizados, entre otros)
  + Sistema inactivo por fallas en los aplicativos o plataformas de TI
  + Errores en copias de seguridad o fallas de restauración
  + Sistema inactivo e inaccesible por falla lógica en los servidores virtuales o actualizaciones erróneas

|  |
| --- |
| Actividades de prevención |

* Disponer procedimientos definidos, documentados y socializados
* Establecer los roles y responsabilidades de los procedimientos
* Definir las políticas y establecer los objetivos para el mejoramiento de los procedimientos
* Garantizar que el procedimiento se ejecute
* Disponer espacios de trabajo cuando sean requeridos y establecer mecanismos para la revisión del DRP
* Verificar la correcta ejecución de copias de seguridad de las máquinas y servicios o sistemas de información críticos
* Diseñar e implementar estrategias para garantizar la continuidad tecnológica
* Hacer pruebas periódicas a los componentes de TI
* Asegurar que los ambientes de producción y contingencia se mantienen idénticos para las aplicaciones y servicios
* Realizar informes de las pruebas realizadas
* Mantener actualizados los manuales operativos, los procedimientos y los instructivos de las aplicaciones

|  |
| --- |
| Equipo de Recuperación DRP del *abreviatura/nombre del sistema de información* |

### Grupo Responsable de la Gestión de Crisis



### Roles y Responsabilidades

*A continuación encontrará una tabla que contiene todos los roles y responsabilidades, diligencie la tabla, analizando y depurando, de modo que la tabla solo conserve aquellas que aplican para este DRP en particular.*

| **ROL** | **ANTES DEL INCIDENTE**  **DRP** | **DURANTE EL INCIDENTE**  **DRP** | **DESPÚES DEL INCIDENTE DRP** |
| --- | --- | --- | --- |
| **Jefe de la Oficina de Tecnología e Informática o quién este delegue** | * Definir el alcance de las pruebas al DRP, si abarcarán a toda la infraestructura o a una parte de esta. | * Monitorear y hacer seguimiento al cumplimiento del Plan Recuperación ante Desastres. * Asignar los recursos necesarios para el análisis, evaluación, definición del plan de acción y ejecución del DRP. | * Informar a los terceros y demás partes interesadas las acciones llevadas a cabo en el DRP enmarcado dentro del Protocolo de Comunicaciones en Crisis para Contingencias – Tecnología. * Realizar seguimiento a la ejecución del DRP y validar las opciones para retornar a la operación normal. |
| **Líder de la Práctica ITIL: Profesional de la Oficina de Tecnología e Informática - OTI** | * Liderar y apoyar la formulación, implementación, seguimiento y evaluación de políticas, estrategias y del DRP. * Asegurar que el procedimiento se encuentra definido, documentado y socializado. * Establecer los roles y responsabilidades del procedimiento. * Definir las políticas del procedimiento y establecer objetivos para el mejoramiento de este. * Solicitar espacios de trabajo cuando sea requerido y establecer mecanismos para la revisión del DRP. * Validar las actividades definidas en la etapa de definición de planes, alcance y políticas para la ejecución de las pruebas a nivel de DRP. * Comunicar el contenido de este procedimiento y todos sus documentos anexos. | * Garantizar que el procedimiento se ejecute. | * Informar a la alta dirección sobre el estado de la recuperación. * Mantener informados a los usuarios finales sobre el impacto y los tiempos estimados de restauración. |
| **Personal de Apoyo en Gestión de Continuidad: Proveedor de Servicios de TI** | * Apoyar la realización de actividades de análisis de riesgos, BIA, estrategias de la continuidad del servicio TI para el Plan de Recuperación de Desastres – DRP sobre los diferentes activos que componen los servicios de TI, bajo las mejores prácticas en valoración y análisis de riesgo. * Apoyar la gestión para la ejecución de los planes de pruebas a nivel de DRP. * Apoyar la actualización del Procedimiento de la Continuidad del Servicio de TI, e identificación y aplicación de las oportunidades que permitan mejorar el desempeño de estos. * Llevar a cabo las revisiones regulares del Plan de Recuperación de Desastres. * Informar el propósito del DRP a las partes interesadas y realizar los informes y recomendaciones requeridas para la mejora el mismo. | * Apoyar a los Profesionales de Continuidad en la ejecución de lo definido en las políticas y procedimientos establecidos para el DRP. | * Propender por el mantenimiento actualizado de toda la documentación técnica para la continuidad del servicio de TI. |
| **Personal especializado en recuperación de los servicios de TI: Profesional de la OTI o Especialista del proveedor de Servicios de Tecnología** |  | * Evaluar el impacto de la afectación en los servicios de TI, en el evento de materialización de un desastre y la aplicación del presente procedimiento en caso de afectación de su servicio. * Cumplir los planes y las políticas de continuidad del servicio de TI necesarios para proteger el desarrollo normal de los servicios que administra en caso de un eventual desastre. * Coordinar la ejecución de las actividades de los planes y procedimientos del DRP, respecto a su servicio. * Mantener informados a las partes interesadas internamente de los avances y cierres de los planes de recuperación del servicio de TI, retorno y cierre del DRP. | * Apoyar el seguimiento a la ejecución del DRP y validar las opciones de retornar a la operación normal de su servicio. |
| **Líder de Seguridad** | * Apoyar actividades de entrenamiento, documentación y actualización del DRP. * Validar las actividades de pruebas del DRP. * Identificar los recursos requeridos para la operación del DRP. | * Proveer soporte a los profesionales especializados. * Notificar al proveedor de Centro de Cómputo Alterno (si aplica). * Gestionar el alistamiento y disponibilidad del Centro de Cómputo Alterno. * Coordinar con los responsables el desplazamiento al Centro de Cómputo Alterno, de los funcionarios que activarán la infraestructura. (Si aplica). * Mantener informado al Jefe de la OTI. | * Actualizar el DRP, de acuerdo con los inconvenientes y oportunidades de mejora encontrados. |

|  |
| --- |
| Activación y Notificación DRP |

### Activación DRP

*En esta sección debe describir el proceso para la activación del DRP del sistema de información en cuestión. Incluya un diagrama de flujo que ilustre el proceso, desde la detección y el reporte del incidente, pasando por la evaluación y las decisiones clave sobre la gravedad del incidente y la necesidad de activar el DRP, hasta la notificación, la validación de sitios alternos, la recuperación de sistemas y la documentación de las lecciones aprendidas.*

*Posteriormente, cada paso del diagrama debe detallarse en una tabla que especifique las actividades correspondientes, los criterios de decisión y las responsabilidades asociadas.*

### Notificación DRP



| **FALLA DATA CENTER SIPI** | | | | |
| --- | --- | --- | --- | --- |
| **No** | **Actividad** | **Descripción** | **Responsable** | **Tiempo** |
| 1 | Verificar conexión al DC principal | El ingeniero verifica el estado de comunicación del canal principal | IT ? | 15 minutos |
| 2 | Decidir ¿Hay Conexión? | Informar mediante correo electrónico y llamada telefónica al proveedor del canal el incidente de no disponibilidad de la comunicación. | IT ? | 15 minutos |
|  | NO Hay Conexión | Ir Actividad 15. | IT ? | 15 minutos |
| 3 | Verificar Plataforma SIPI |  | IT ? | 15 minutos |
| 4 | Decidir ¿SIPI Operando en DC principal? | Ir Actividad 14. | IT ? | 15 minutos |
|  | SIPI NO Operando en DC principal | En caso de que no se logre la comunicación con el centro de datos principal, es necesario comunicar por correo electrónico y llamada telefónica al proveedor para el levantamiento de máquinas en el centro de datos alterno. | IT ? | 15 minutos |
| 5 | Verificar Servidores SIPI |  | IT ? | 15 minutos |
| 6 | Decidir ¿Servidores SIPI Operando? | El ingeniero solicita al proveedor, la verificación de las máquinas virtuales para conocer su estado de funcionalidad.  Ir Actividad 3. | IT ? | 30 minutos |
|  | Servidores SIPI NO Operando | Comunicar al proveedor por correo electrónico, la restauración de las máquinas virtuales y la data en el servidor alojado en el centro de datos alterno. | IT ? | 30 minutos |
| 7 | Verificar Datos RPO SIPI | De acuerdo con la última copia de seguridad, se requiere validar la disponibilidad de los sistemas de información y la pérdida de información. | IT ? | 2 hora |
| 8 | Notificar Grupo DRP SIPI | Informar a los líderes de proceso, la pérdida de información de acuerdo con la última copia de seguridad restaurada, con el fin de iniciar actividades manuales de recuperación de la información. | Director OTI | 30 minutos |
| 9 | Informar Mesa Servicios | El proceso de IT inicia las actividades críticas como la atención de solicitudes a través de la mesa de ayuda. | Director OTI | 30 minutos |
| 10 | Recuperar SIPI | Apoyar al personal para iniciar las actividades críticas de cada proceso. Brindar soporte de accesibilidad con los sistemas de información. | Equipo Mesa Servicios | 1 hora |
| 11 | Decidir ¿Retornar a la Normalidad? |  | Director OTI | 30 minutos |
|  | NO Hay Normalidad | Ir Actividad 17. | Director OTI | 30 minutos |
| 12 | Procesos de Normalidad | El proceso de retorno se debe realizar en horario que no afecte las actividades, así como una planeación detallada para evitar pérdida de información o la duplicidad de la misma. | Director OTI | 2 horas |
| 13 | Verificar DC Principal |  | IT ? | 15 minutos |
| 14 | <FIN> Falla DC SIPI | Termina el procedimiento |  |  |
|  | | | | |
| 15 | Validar conexión auxiliar | Verificar la conexión de contingencia | IT ? | 15 minutos |
| 16 | Decidir ¿Hay Conexión? | Ir Actividad 3. | IT ? | 15 minutos |
|  | NO Hay Conexión | Ir Actividad 17. | IT ? | 15 minutos |
| 17 | Activar DRP en DC Alterno | Ir Actividad 2. | IT ? | 15 minutos |

|  |
| --- |
| 1. **PLATAFORMA TECNOLÓGICA DEL *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** |

|  |
| --- |
| Infraestructura Crítica del *abreviatura/nombre del sistema de información* |

*En esta sección debe describir la infraestructura crítica del sistema de información, proporcionando un panorama detallado de los componentes tecnológicos esenciales que soportan su funcionamiento.*

*Incluya un diagrama de arquitectura tecnológica.*

*En el texto, explique cómo estos elementos interactúan para garantizar la operatividad del sistema. Si aplica, describa restricciones actuales, como la necesidad de adquirir licencias específicas, y presente recomendaciones justificadas para optimizar la infraestructura o reducir costos, como en el caso de licencias limitadas frente a ilimitadas.*

|  |
| --- |
| Servidores del *abreviatura/nombre del sistema de información* |

*Diligencie la siguiente tabla para documentar este apartado:*

|  |  |  |
| --- | --- | --- |
| **DESCRIPCION** | **NOMBRE DE LA MAQUINA** | **DIRECCION**  **IP** |
|  |  |  |

|  |
| --- |
| Arquitectura del *abreviatura/nombre del sistema de información* - IFX |

*Incluya un diagrama de infraestructura de TI que represente la estructura del sistema información alojado en el IFX, mostrando los diferentes componentes, como servidores, bases de datos, balanceadores de carga y su interconexión.*

|  |
| --- |
| Arquitectura Bochica |

*Incluya un diagrama de infraestructura de TI que represente la estructura del sistema información alojado en Bochica, mostrando los diferentes componentes, como servidores, bases de datos, balanceadores de carga y su interconexión. Además, para la sección describa el contenido del diagrama en la siguiente tabla:*

|  |  |  |  |
| --- | --- | --- | --- |
| **DESCRIPCIÓN** | **NOMBRE DE LA MAQUINA** | **DIRECCIÓN**  **IP** | **DIRECCIÓN IP BOCHICA** |
|  |  |  |  |

|  |
| --- |
| Caracterización Servidores del *abreviatura/nombre del sistema de información* |

*Para caracterizar los servidores involucrados en este sistema de información, diligencie la siguiente tabla:*

| **#** | **SISTEMA** | **Nombre del servidor** | **CPU** | **Disco Duro** | **RAM** | **Detalle Sistema Operativo** | **Observaciones** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

|  |
| --- |
| Arquitectura de Aplicaciones y Servicios del *abreviatura/nombre del sistema de información* |

*Incluya un diagrama de aplicación que represente cómo se organizan y se comunican los diferentes componentes del sistema de información e indique los servicios que interactúan y cómo se conectan entre sí. Además, para la sección además diligencie la siguiente tabla, una por cada aplicación:*

| **INFRAESTRUCTURA GENERAL DE LA APLICACIÓN** | | |
| --- | --- | --- |
| **No** | **Servicio** | **URL** |
|  |  |  |

| **OTROS SERVICIOS NECESARIOS** | | |
| --- | --- | --- |
| **No** | **Detalle** | **Servicio Requerido** |
|  |  |  |

|  |
| --- |
| 1. **ACTIVIDADES DE GESTIÓN DE CRISIS** |

El/La Jefe de la OTI Informa a los terceros y demás partes interesadas las acciones llevadas a cabo en el DRP enmarcado dentro del Protocolo de Comunicaciones en Crisis para Contingencias - Tecnología, el cual se encuentra inmerso dentro del Plan de Comunicaciones.

Las actividades necesarias para el manejo de una crisis que pueda afectar la imagen y operación de la Superintendencia de Industria y Comercio son:

El/LA Jefe de la Oficina de Tecnología e Informática debe comunicar a la Alta Dirección lo siguiente:

* Sistemas y servicios afectados
* Resultados del diagnóstico
* Acciones realizadas
* Tiempo estimado para normalización
* Riesgos a los que está expuesta la entidad por el desastre presentado, y las alternativas disponibles
* Decisiones que debe tomar la alta dirección.

La Alta Dirección evalúa la crisis y el impacto para la entidad, además define las acciones para enfrentar la crisis. Además, debe comunicar por medio de los funcionarios delegados o voceros la crisis a nivel interno y externo considerando:

* ¿Qué información concreta se tiene sobre el incidente presentado, diagnóstico y tiempo de solución?
* ¿Qué información está en proceso de verificación e investigación?
* ¿Qué información válida se puede comunicar inmediatamente (mensaje)?
* ¿Qué información se debe manejar al interior de la entidad?
* ¿Quiénes fueron afectados por la crisis (audiencia)?
* ¿Qué otras audiencias deberían saber sobre la crisis?
* ¿Cómo se comunicará la información a los interesados o afectados (medio)?

Basarse en los principios de la comunicación así:

* **Informar rápida y periódicamente:** Ante una situación de crisis de alto impacto, la entidad debe establecerse como fuente primaria de información, asimismo, debe comunicar periódicamente la evolución de la atención de la crisis para evitar malos entendidos, especulaciones y rumores. Estos elementos le permitirán generar confianza y credibilidad con sus audiencias.
* **Decir la verdad**: Ser honestos en los comunicados, sin embargo no significa transmitir TODA la información, sólo aquella que es suficiente para generar confianza y tranquilidad en la audiencia. Podrá existir información confidencial que deberá ser tratada como tal y no se necesite transmitir a los interesados.
* **Emitir reportes lo más exactos posible**: Publicar la información que se tiene disponible, siempre y cuando ésta haya sido validada. No especular, adivinar ni presentar situaciones hipotéticas.

Considerar en la comunicación de la crisis las siguientes audiencias:

* Sociedades inspeccionadas, vigiladas y/o controladas
* Usuarios externos de los productos y/o servicios de la entidad.
* Funcionarios
* Opinión Pública
* Gobierno y Autoridades
* Líderes de Opinión
* Contratistas y Proveedores

Monitorear continuamente la crisis y evaluar:

* ¿Qué información circula en los medios de comunicación?
* ¿Qué información circula a nivel interno?
* ¿Qué impacto sobre la crisis tiene la información que está circulando en los medios?
* ¿Se requerirá realizar nuevos comunicados?

|  |
| --- |
| 1. **MANTENIMIENTO DEL DRP *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** |

|  |
| --- |
| Actualización manual DRP *abreviatura/nombre del sistema de información* |

Es responsabilidad del Líder del Grupo de Trabajo de Informática Forense y Seguridad Digital la actualización de las nuevas versiones al DRP, y su respectiva comunicación a todos los colaboradores involucrados en el DRP.

El Plan de Recuperación ante Desastres debe ser revisado en cumplimiento de la normatividad vigente y como mínimo una vez al año.

También debe ser actualizado si se presenta:

* Cambios importantes en la infraestructura, las personas del equipo del proceso de IT o la infraestructura tecnológica.
* Cambios de proveedores tecnológicos.
* Hallazgos de revisiones independientes.
* Pruebas fallidas del plan.
* Productos y servicios nuevos o eliminados.
* Cuando los resultados de las pruebas requieren actualización del DRP o sus procedimientos.
* Cuando hay cambios en el personal que operaría el DRP.
* Cuando los resultados de auditorías así lo indican.

|  |
| --- |
| 1. **PLAN DE PRUEBAS *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*** |

|  |
| --- |
| Tabla de Errores |

OMPI: Se debe tener en cuenta que puede haber algunas restricciones de IP entrantes por parte de la OMPI, si la SIC tiene una nueva dirección IP pública para la plataforma de contingencia se debe notificar.

|  |
| --- |
| Contingencia y Soporte |

*Se debe incluir una lista de las personas a las cuales el usuario puede solicitar apoyo en caso de que el sistema presente algún problema.*

Especialistas: Los especialistas definidos de acuerdo con las aplicaciones e infraestructura críticas que se encuentran relacionados en el documento: **“Catalogo de Sistemas de Información SIC 2020”**, para el caso de los especialistas la información se encuentra recopilada en el archivo “Matriz de escalamiento” y la información de los especialistas de los diferentes grupos se encuentra documentada al interior de la OTI. Nota: Una misma persona puede cumplir varios roles.

### Encendido del *abreviatura/nombre del sistema de información* en el Data Center Alterno (Bochica) *(Este punto es solo si aplica)*

El Procedimiento para encender el ***abreviatura/nombre del sistema de información*** totalmente, el orden en las actividades es importante y necesario. Así:

| **ENCENDIDO DEL *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*  EN DATACENTER ALTERNO** | | |
| --- | --- | --- |
| **No** | **Actividad** | **Descripción** |
|  | *Describa en orden y paso a paso lo que se debe hacer.* |  |

|  |
| --- |
| Plan de Pruebas |

Las pruebas de operación del Data Center Alterno deben ser realizadas cada seis meses, para garantizar el correcto funcionamiento del *abreviatura/nombre del sistema de información* ante un desastre de disponibilidad.

Para realizar este proceso se deben adelantar las siguientes actividades:

*Para describir las actividades que se deben adelantar, por favor, diligencie en orden la siguiente tabla, desde la complementación del título y agregue tantas filas como sea necesario, diligenciando una responsabilidad por fila.*

|  |
| --- |
| **RFC - PLAN DE PRUEBAS DRP *ABREVIATURA/NOMBRE DEL SISTEMA DE INFORMACIÓN*  – *MES-AÑO*** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **ACTIVIDAD** | **NOMBRE RESPONSABLE** | **CARGO RESPONSABLE** | **EMPRESA** | **FECHA PROPUESTA DE EJECUCIÓN dd/mm/aa** | **HORA PROPUESTA DE INICIO DE EJECUCIÓN** | **HORA PROPUESTA DE FIN DE EJECUCIÓN** | **DURACIÓN** | **OBSERVACIONES** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| **ROLLBACK *(Sí aplica, de lo contrario eliminar la tabla y el título)*** | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
| **No.** | **ACTIVIDAD** | **NOMBRE RESPONSABLE** | **CARGO RESPONSABLE** | **EMPRESA** | **FECHA PROPUESTA DE EJECUCIÓN dd/mm/aa** | **HORA PROPUESTA DE INICIO DE EJECUCIÓN** | **HORA PROPUESTA DE FIN DE EJECUCIÓN** | **DURACIÓN** | **OBSERVACIONES** |
|  |  |  |  |  |  |  |  |  |  |

|  |
| --- |
| 1. **GLOSARIO DE TÉRMINOS** |

*En esta sección se incluirá una lista con el significado de los términos, conceptos o tecnicismos, usados en este manual y que no son del dominio público.*

*Agregar siglas y definiciones técnicas del sistema de información.*

|  |
| --- |
| 1. **ANEXOS** |

|  |
| --- |
| Matriz de Escalamiento |

Matriz de escalamiento con los datos de los especialistas requeridos en caso de un desastre.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MATRIZ DE ESCALAMIENTO** | | NIVEL 1 | |  |
| **LINEA** | **ROL** | **RESPONSABLE** | **CORREO 1 - SIC** | **CORREO 2 - Carvajal** |
| SEGUIMIENTO Y CONTROL | Líder Técnico | Manuel Alejandro Muñoz Jiménez | [lider.tecnico@sic.gov.co](mailto:lider.tecnico@sic.gov.co) | [manuel.munoz@carvajal.com](mailto:manuel.munoz@carvajal.com) |
| Líder de servicio y Gestión Operativa | Emerson Camelo Tovar | lider.servicio@sic.gov.co | [emerson.camelo@carvajal.com](mailto:emerson.camelo@carvajal.com) |
| Líder DC/NOC/SOC | Jhonny Guevara Guevara | N/A | Jhonny.Guevara@carvajal.com |
| Administrador Aranda - Mejoramiento funcionalidades Aranda | Hermes Julián Gutiérrez Briñez | N/A | hermes.gutierrez@carvajal.com |
| Administrador inventarios (equipos cómputo - servicios impresión), licenciamiento, logística | Daniel Hernán Basutista | [c.incarvajal@sic.gov.co](mailto:c.incarvajal@sic.gov.co) | [daniel.bautista2@carvajal.com](mailto:daniel.bautista2@carvajal.com) |
| Yuly Alexandra González Agudelo | [c.incarvajal@sic.gov.co](mailto:c.incarvajal@sic.gov.co) | [yuly.gonzaleza@carvajal.com](mailto:yuly.gonzaleza@carvajal.com) |
| Documentador TI | Ana Cristina Figueredo | documentadorti@sic.gov.co | [ana.figueredo@carvajal.com](mailto:ana.figueredo@carvajal.com) |
| GESTORES ITIL, CALIDAD, INVENTARIOS Y LOGISTICA DE PROVEEDORES | Gestores ITIL V3 (Requerimientos, Accesos y Problemas) | Alexander Castro | N/A | [alexander.castroT@carvajal.com](mailto:alexander.castroT@carvajal.com) |
| Gestores ITIL V3 (ANS) | Deisy Nathaly Ramírez | N/A | [deisy.ramirezl@carvajal.com](mailto:deisy.ramirezl@carvajal.com) |
| Gestores ITIL V3 (Incidentes, Eventos y Disponibilidad) | Ana Isabel Caicedo | N/A | ana.caicedo@carvajal.com |
| Gestores ITIL V3 (Conocimiento Catálogo y Portafolio) | Karol Giveth Palencia | N/A | karol.palencia@carvajal.com |
| Gestor Diseño, Estrategia y Transición de Servicios | Luis Alejandro Martínez | N/A | Luis.MartinezT@carvajal.com |
| Gestor Seguimiento y Control Operación de Servicios | Deisy Ramírez | N/A | [deisy.ramirez@carvajal.com](mailto:deisy.ramirez@carvajal.com) |
| Gestor de Mejora Continua | Kelly Yohana Orozco | N/A | [kelly.orozcoc@carvajal.com](mailto:kelly.orozcoc@carvajal.com) |
| Gestor Riesgos V4 / Proyectos V4 | Adriana Marcela Dueñas | N/A | adriana.duenas@carvajal.com |
| Gestor de Infra y Plataforma v4 / Desarrollo y Gestión de SW v4 / Capacidad | Luis Alejandro Martínez | N/A | Luis.MartinezT@carvajal.com |
| Gestor de Activos y Configuración | Adriana Marcela Dueñas | N/A | adriana.duenas@carvajal.com |
| Gestores ITIL V3 (Cambios, Liberación y Entregas) | Fabian Camilo Tovar Aldana | N/A | fabian.tovar@carvajal.com |
| Analista de Calidad | Karen Tatiana Garzón | N/A | [karen.garzon@carvajal.com](mailto:karen.garzon@carvajal.com) |
| Coordinador Mesa de Servicios y soporte en sitio | Elizabeth Aguilar Sáenz | N/A | [Elizabeth.Aguilar@carvajal.com](mailto:Elizabeth.Aguilar@carvajal.com) |
| MESA DE SERVICIO, SOPORTE EN SITIO E INFRAESTRUCTURA | Especialista Linux | John Jairo Cotacio Melo | dc.linux@sic.gov.co | [john.cotacio@carvajal.com](mailto:john.cotacio@carvajal.com) |
| Administración de correo | Jorge Eliecer Celis Fajardo | [dc.correo@sic.gov.co](mailto:dc.correo@sic.gov.co) | [jorge.celis@carvajal.com](mailto:jorge.celis@carvajal.com) |
| Especialista Admin. Base de datos | William Eduardo Hurtado Salcedo | dc.dba@sic.gov.co | [william.hurtado@carvajal.com](mailto:william.hurtado@carvajal.com) |
| Especialista Windows | Christian Darío Rodríguez Salinas | dc.windows@sic.gov.co | [christian.rodriguezs@carvajal.com](mailto:christian.rodriguezs@carvajal.com) |
| Especialista Storage y Backup | Wilman Augusto Marín Mancera | dc.storage@sic.gov.co | [wilman.marin@carvajal.com](mailto:wilman.marin@carvajal.com) |
| Especialista OpenShift | Wilman Augusto Marín Mancera | dc.openshift@sic.gov.co | [wilman.marin@carvajal.com](mailto:wilman.marin@carvajal.com) |
| Especialista Jboss | Hernán Sánchez Álvarez | dc.jboss@sic.gov.co | [hernan.sanchez@carvajal.com](mailto:hernan.sanchez@carvajal.com) |
| Especialista Informix - Solaris | Hermann Jiménez | dc.informix@sic.gov.co | [hermann.jimenez@carvajal.com](mailto:hermann.jimenez@carvajal.com) |
| Especialista Virtualización y Nube | Ronald Fernando Avellaneda Arévalo | dc.virtualizacion@sic.gov.co | [ronald.avellaneda@carvajal.com](mailto:ronald.avellaneda@carvajal.com) |
| Seguridad Informática / SOC | Analistas SOC | N/A | N/A | [soc@carvajal.com](mailto:soc@carvajal.com) |
| Especialista Redes | Néstor Raúl Gallego Villa | [dc.redes@sic.gov.co](mailto:dc.redes@sic.gov.co) | [nestor.gallego@carvajal.com / redestisic@carvajal.com](mailto:redestisic@carvajal.com%20/) |
| Especialista de Seguridad Y Antivirus | N/A | N/A | [seguridadtisic@carvajal.com](mailto:seguridadtisic@carvajal.com) |
| NOC / DC | Analistas NOC | N/A |  | [CarvajalTSColombiaDataCenterBogota@carvajal.com](mailto:CarvajalTSColombiaDataCenterBogota@carvajal.com) |
| Administrador Herramienta Monitoreo (PRTG) | Rocío Lemus Acosta | N/A | [GestionHerramientas@carvajal.com](mailto:GestionHerramientas@carvajal.com) |
| Administrador Herramienta Monitoreo (PRTG) | Ricardo Medina Castillo | N/A | [GestionHerramientas@carvajal.com](mailto:GestionHerramientas@carvajal.com) |

Fin del documento