**PLAN DE CONTINUIDAD DEL NEGOCIO, EN CASO DE SITUACIONES INESPERADAS**

1. **Objetivo**

Evitar interrupciones a los procesos comerciales del negocio como consecuencia de fallas o desastres.

1. **Definiciones**

**Plan de continuidad del negocio** (BCP-Business Continuity Plan, DRP): Un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio de PINTURAS INDUSTRIALES.

**Plan de Contingencia**: Es un subconjunto de un plan de continuidad de negocio (BCP,DRP), que contempla como reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los sistemas informáticos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de software o hardware, errores humanos, intrusión etc.

**Plan de recuperación frente a desastres** (DRP): Es aquella parte del plan de contingencia y del plan de continuidad de negocio (BCP), que aborda aquellas contingencias que, por su gravedad, no permiten continuar prestando el servicio desde el centro local y debe continuarse el servicio desde un nuevo centro. Este plan debe contemplar la vuelta atrás cuando, tras arreglar las consecuencias del desastre, el servicio pueda ser reanudado en el centro local.

1. **PLAN DE CONTINUIDAD DE NEGOCIO (BCP)**

Contar con un **Plan de Continuidad de Negocio (BCP)**, pensado y desarrollado para garantiza la prestación del servicio a la cual nuestros clientes están acostumbrados, independientemente de las situaciones que se presenten. Este Plan tiene las siguientes características:

* **Seguro empresarial**: A través de una correcta planeación, una buena administración del cambio tecnológico y que de manera constante sea probado, se puede garantizar que el Plan, ya sea de **Continuidad de Negocio** o **Recuperación de Desastres** sean seguros.
* **Automatizado**: contamos con sedes externas, que tienen la plataforma tecnológica adecuada y con las respectivas [copias de seguridad](https://www.valoradata.com/vd-backup/) de la Información clave del negocio, ya que ante un desastre lo primero que sufre es la infraestructura física y tecnológica además de dejar inoperantes a sus empleados.
* **Justificable**: Las soluciones planteadas en los Planes no son sólo útiles para las **Contingencia**s reduciendo **riesgos,** sino que fortalecen las operaciones diarias y mejoran los procesos existentes.

**Plan de Recuperación de Desastres (DRP)**

Un **Plan de Recuperación de Desastres (DRP)**, se refiere a la recuperación de todo lo referente a la tecnología. Representa las actividades que se realizaran en un tiempo especificado en caso de que alguna **contingencia**, amenace o detenga el funcionamiento de los recursos tecnológicos de la empresa, permitiendo recuperar los servicios críticos

Este plan involucra los siguientes factores:

* **La Agenda telefónica o árbol telefónico**, es decir, la lista de contactos con sus respectivos números telefónicos de los empleados para notificarles al personal clave sobre el problema y delegar funciones orientadas al Plan de Recuperación.
* **Reservas de**[**Copias de Seguridad**](https://www.valoradata.com/vd-custody/): Pueden ser de manera física, en dispositivos que deben encontrarse fuera del sitio del desastre y si son copias de seguridad remotas se requiere de una conexión de red o Internet. Primordialmente la Información clave del Negocio
* **Los clientes**, para evitar el pánico e incertidumbre se deben notificar a los clientes del problema.
* **Personal calificado y entrenado para desastres**, disponer de un sistema de apoyo, donde los empleados conscientes de la situación trabajen por más horas y arduamente.

El **Plan de Continuidad de Negocio (BCP)** detalla las responsabilidades de cada empleado ante el desastre cualquiera sea su naturaleza, y la manera de mantener la comunicación entre ellos.  Para elaborar el **Plan** debe tomarse en cuenta los siguientes aspectos:

* **Flexibilidad**, para adaptarse a cualquier riesgo que pueda ocurrir en la organización, para ello se deben identificar las posibles situaciones de **riesgos**, internos y externos que afecten la **Continuidad del Negocio**, destacando las posibles consecuencias que se generarán de cada situación.
* **Asertividad**, para dar respuesta a cada situación, detallando la forma de responder a la empresa con acciones específicas, recursos y responsables de llevarlas a cabo.
* **Listado de contactos actualizados**: tener una base de datos, preferiblemente externa: datos de clientes, empleados, proveedores. **Organización**, establecer el organigrama para la toma de decisiones durante el tiempo de la **Contingencia**

.

## ESTRATEGIAS DE CONTINUIDAD

Una estrategia de continuidad es un mecanismo que permite la recuperación y continuidad de las funciones críticas de una organización frente a un desastre o una interrupción mayor. Son consideradas como estrategias no sólo los recursos y actividades requeridas frente a la interrupción, sino los requeridos para mitigar la probabilidad de ocurrencia y el impacto de la interrupción.

Para definir las estrategias de continuidades posibles o viables, de manera efectiva y eficiente, se debe contar con un entendimiento sobre los siguientes aspectos:

1. Tiempos y puntos objetivo de recuperación requeridos para los procesos críticos.
2. Procesos críticos a soportar
3. Porcentaje aceptable de degradación de la operación del proceso.
4. Aspectos de carácter jurídico que se deben cumplir según la naturaleza del proceso al momento de implementar una estrategia de recuperación.
5. Resultados del análisis de riesgos y las alternativas de tratamiento de riesgo a implementar sobre los activos asociados a los procesos.
6. Amenazas posibles a los activos de los procesos.
7. Vulnerabilidades existentes en los activos de los procesos.

El propósito de esta fase consiste en seleccionar las estrategias de recuperación o continuidad, orientadas a brindarle confiabilidad a los servicios, considerando los resultados, la evaluación de riesgos y complementado lo anterior, con la realización de un análisis cuantitativo de los elementos requeridos para la recuperación.

Parte del desarrollo abarcó la definición de los escenarios de interrupción, las amenazas que los pudieran generar y las diferentes alternativas operativas para enfrentar una posible materialización. En la siguiente tabla se visualiza la información referente:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ESCENARIOS | | | | |
|  | Infraestructura No Disponible | TI No  Disponible | Recurso Humano No Disponible | Proveedor No Disponible | Información No disponible |
| AMENAZAS | * Incendio, inundación, episodios de violencia, terremotos * Cierre Parcial | * Falla Eléctrica * Incendio * Inundación * Terremoto * Falla tecnológica | * Incendio * Actos de violencia * Terremoto * Cierre Parcial * Ausencia, retiro, muerte de un funcionario | * Falla Eléctrica * Incendio * Inundación * Terremoto * Falla tecnológica | * Falla Eléctrica * Incendio * Inundación * Sismo o Terremoto * Fallas tecnológicas en: Comunicaciones, Hardware, Software, Bases de Datos * Error Humano * Hurto o Robo |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ESCENARIOS | | | | |
|  | Infraestructura No Disponible | TI No  Disponible | Recurso Humano No Disponible | Proveedor No Disponible | Información No disponible |
| ALTERNATIVAS OPERATIVAS | * Trabajo a distancia * Acuerdo con Terceros * Respaldo entre sedes * Centro de Trabajo Alterno | * Estrategia DRP | * Definición de la   Estructura de Recuperación en Cascada (ERC)   * Capacitación * Rotación * Documentación de procedimientos | * Definir proveedores alternos * Definir Acuerdos de   Niveles de Servicio específicos para BCM. | * Respaldo de la información clave del proceso (Backup) * Proveedores y/o medios Alternos para el servicio de comunicación |

La siguiente es la relación de alternativas operacionales que tiene la organización, para recuperar la funcionalidad de sus procesos críticos en términos de la ausencia de alguno(s) de sus recursos claves, estas estrategias pueden permitir la continuidad de sus operaciones más importantes en un nivel aceptable y buscan principalmente cumplir y satisfacer los requerimientos del producto solicitado por sus clientes, después de un evento de interrupción:

|  |  |  |
| --- | --- | --- |
| ESCENARIO DE  INTERRUPCIÓN | AMENAZAS | ALTERNATIVAS OPERATIVAS |
|  | * Huelga de Colaboradores * Pandemia * Intoxicación Colectiva * Indisposición de Colaboradores (Ausencia, retiro o muerte) | * Definición de árboles de llamada. * Capacitación * Rotación * Documentación de procedimientos |
|  | * Incendio * Inundación * Actos de Violencia * Sismo o Terremoto * Asonadas * Fugas de gas * Explosión | * Teletrabajo o home work * Acuerdo con terceros * Respaldo entre sedes (planta de producción) * Centro de Trabajo Alterno trabajo alterno para procesos administrativos |

|  |  |  |
| --- | --- | --- |
| ESCENARIO DE  INTERRUPCIÓN | AMENAZAS | ALTERNATIVAS OPERATIVAS |
|  | * Falla Eléctrica * Incendio * Inundación * Sismo o Terremoto * Fallas tecnológicas en: Comunicaciones, Hardware, Software, Bases de Datos | * Estrategia DRP |
|  | Falla Eléctrica   * Incendio * Inundación * Sismo o Terremoto * Fallas tecnológicas en: Comunicaciones, Hardware, Software, Bases de Datos * Error Humano * Hurto o Robo | * Respaldo de la información clave del proceso (Back Up) * Proveedores y/o medios Alternos para el servicio de comunicación |
|  | No disponibilidad del Proveedor por eventos propios de su operación:   * Falla Eléctrica * Incendio * Inundación * Huelgas o Asonadas * Pandemias * Actos de Violencia * Sismo o Terremoto * Fallas tecnológicas * No disponibilidad de sus Proveedores | * Definir proveedores alternos del servicio * Definir Acuerdos de Niveles de Servicio específicos para BCM |