POLITICA DE CONTINUIDAD Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

EMPRESA DE RECURSOS TECNOLÓGICOS

INTRODUCCIÓN

El riesgo es la probabilidad de que se presente un peligro y que este último traiga consecuencias para la empresa. Los peligros por si solos no representan una amenaza para la operación, pero si a este se suma una vulnerabilidad, ese peligro se convierte en un riesgo para la empresa, es decir que existe la probabilidad de que ocurra un desastre.

Los riesgos se miden de acuerdo a la magnitud de los daños que pueden ocasionar y a la probabilidad de que ocurran, de tal forma la probabilidad de que ocurra una consecuencia por cierto evento dependerá de la probabilidad de que el evento ocurra y del tiempo de exposición del bien (material, humano, etc.) a tal factor de riesgo.

Toda organización está expuesta a peligros de diferente índole que representan diferentes niveles de riesgo debido al impacto que pueden llegar a tener y a la frecuencia con que está expuesta la organización a estos peligros. Por este motivo evaluar los posibles riesgos dentro de la empresa es muy importante, ya que le permite identificar y evaluar los riesgos para prevenirlos, protegerse contra ellos o mitigar sus consecuencias.

La Empresa de Recursos Tecnológicos reconoce que existen riesgos que una vez se presenten tienen una probabilidad de originar accidentes que amenacen la normal operación de la empresa, la cual tiene la necesidad de recuperarse en el menor tiempo posible garantizando la continuidad de sus operaciones.

OBJETIVOS

Objetivo General

Asegurar que el área de servicios telemáticos de la Empresa de Recursos Tecnológicos esté preparada para mitigar y atender los peligros que se presenten, dando continuidad a los servicios críticos que se desarrollan al interior del área.

Objetivos Específicos

- Conocer los peligros a los que está expuesta el área de Servicios Telemáticos de la Empresa de Recursos Tecnológicos.

- Restaurar de forma ágil y rápida las operaciones afectadas en caso de presentarse una situación de riesgo.

CAUSAS DE INTERRRUPCIÓN

Los planes de contingencia se definen de acuerdo con las causas de las posibles interrupciones y a partir de ellas se relacionan las acciones a seguir en caso que las mismas se presenten.

Dependiendo del alcance o impacto de una contingencia se distinguen las siguientes situaciones:

Incidente: Situación o evento imprevisto, potencialmente peligroso o dañino, que no tiene como resultado lesiones personales, daños ambientales u otras pérdidas.

Accidente: Situación o evento imprevisto, potencialmente peligroso o dañino, que tiene como resultado lesiones personales reales, daños ambientales u otras pérdidas.

Emergencia: Situación o evento imprevisto que exige la participación de servicios públicos de emergencia como policía, bomberos, unidades de servicio médico o autoridades de regulación medioambiental.

El Plan de Contingencias es un programa de tipo predictivo, preventivo y reactivo con una estructura estratégica, desarrollado para el control de una emergencia que se produzca, con el propósito de reducir los riesgos del personal.

1. Plan de Contingencia

El objetivo de un plan de contingencia para las Tecnologías de Información y Comunicación es definir las acciones a realizar para proporcionar continuidad y recuperación en los servicios que proporciona el área de servicios telemáticos a la empresa, dentro de los parámetros que permitan los recursos disponibles.

El plan de contingencia constará de dos fases principales, la primera mostrará las amenazas con posibilidad de ocurrencia alta y que son críticas para la continuidad de operación de los servicios que brinda el área de servicios telemáticos a la empresa y la segunda definirá las acciones a seguir para la recuperación de las operaciones.

1.1. Actividades Asociadas

Las actividades consideradas en este documento son:

- Análisis de Riesgos
- Medidas Preventivas
- Previsión de Desastres
- Plan de Respaldo
- Plan de Recuperación

2. Análisis de Riesgos

De acuerdo a las operaciones de la empresa y de los bienes y servicios que proporciona el área de servicios telemáticos, se han identificado los siguientes problemas críticos:

- Falla en comunicación a Internet
- Falla en comunicación entre inmuebles
- Falla en comunicación de voz
- Falla en el suministro de energía
- Falla en hardware y/o software de servidores
- Falla en aplicaciones
- Virus Informático

2.1. Bienes susceptibles de daño

La infraestructura, aplicaciones e información vulnerable se muestran a continuación:

a) Infraestructura

- Enlace a Internet
- Firewall
- Enlace de comunicación de voz y datos entre inmuebles
- Servidores
- Conmutadores telefónicos
- Unidades de Respaldo de Energía

b) Aplicaciones

- Sistema
  - Presupuesto
  - Tesorería
  - Adquisiciones
  - Activo Fijo
  - Almacén
  - Nómina
  - Personal
  - Capacitación
  - Incidencias
- Sistema Programático
- Sistema de Eventos

c) Información

- Bases de datos de aplicaciones en servidores
- Configuración de usuarios de correo electrónico en servidor
- Directorio activo

2.2. Daños

Dentro de los posibles daños se pueden contemplar:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, ya sea por causas naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, como cambios de claves de acceso, o eliminación de información.

2.3. Prioridades

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los servicios que pierden en el acontecimiento.

RIESGO: FALLA EN APLICACIONES Y SISTEMAS		
IMPACTOS	**CRITICIDAD**	**TIEMPO RECUPERACIÓN**
1. Aplicaciones		**4 horas**
• Nomina • Tesorería • Activos Fijos • Usuarios externos sin acceso a la página WEB de la empresa	Alta Media Media Media	
2. Bases de datos		**4 horas**
• Perdida de información de la base de datos	Alta	
3. Virus		**2 horas**
• Perdida de información o fallas en equipos	Alta	

RIESGO: FALLA EN INFRAESTRUCTURA		
IMPACTOS	**CRITICIDAD**	**TIEMPO RECUPERACIÓN**
1. Enlace de internet		**4 horas**
• Usuarios internos sin acceso a internet	Alta	
• Usuarios externos sin acceso a correo electrónico	Media	
• Usuarios externos sin acceso a la página WEB de la empresa	Media	
2. Firewall		**2 horas**
• Usuarios sin acceso a internet y correo electrónico	Alta	
3. Enlace entre inmuebles		**4 horas**
• Usuarios del inmueble sin acceso a internet y correo electrónico	Media	
• Usuarios sin comunicación de voz	Media	
• Usuarios sin acceso a carpetas y dispositivos compartidos	Baja	
4. Router frontera		**1 hora**
• Usuarios sin acceso a internet	Alta	
5. Servidores de aplicaciones		**4 horas**
• Usuarios internos sin acceso a las herramientas	Alta	
• Usuarios internos sin acceso a correo electrónico	Media	
• Usuarios internos sin acceso al dominio	Alta	
6. Servidor WEB		**2 horas**
• Usuarios sin acceso a la página WEB de la empresa	Media	
7. Servidor MAIL		**2 horas**
• Usuarios sin acceso a correo electrónico	Media	
8. Conmutadores o plantas telefónicas		**2 horas**
• Usuarios sin comunicación telefónica	Alta	
9. Suministro de energía		**2 horas**
• Usuarios internos sin acceso a sus equipos de cómputo	Alta	
• Usuarios internos sin acceso a internet	Alta	
• Usuarios internos sin acceso a correo electrónico	Media	
• Usuarios internos sin acceso a las herramientas	Media	

2.4. Fuentes de daño

Las amenazas que pudieran tener los bienes y servicios que proporciona la Subgerencia Técnica son:

a) Hackeo – Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

b) Virus Informático – Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso.

c) Falla en infraestructura:

- Falla en servidor de aplicaciones y datos, tanto en su(s) disco(s) duro(s) como en el procesador central
- Falla en elementos activos o cableado de red
- Falla en Router o Firewall

d) Falla de Software – Falla en el sistema operativo o cualquier software instalado en los servidores que de soporte a la operación de los servicios.

e) Errores Humanos (Falla de personal clave) – Se considera personal clave aquel que cumple una función vital en el flujo de procesamiento de datos u operación de la Subgerencia Técnica:

- Personal del área
- Soporte Técnico
- Usuarios de Sistemas Críticos

Pudiendo existir los siguientes inconvenientes:

- Enfermedad o accidentes
- Renuncias
- Otros imponderables

f) Desastres Naturales:

- Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos computacionales).
- Inundaciones causadas por falla en los suministros de agua.
- Fallas en los equipos de soporte:
  - Por causas de agresividad en el ambiente
  - Por fallas de la red de energía pública por diferentes razones
  - Por fallas en los equipos de acondicionamiento atmosférico necesarios para una adecuada operación de los equipos computacionales más sensibles
  - Por fallas en el tendido físico de la red local

g) Proveedores con Fallas Técnicas – Servicios contratados con terceros, con ocurrencia de fallas por diferentes razones ajenas al manejo por parte de la Empresa.

h) Errores en Bases de Datos – Estas deben considerarse como parte de la infraestructura tecnológica, ya que los manejadores de bases de datos son el soporte para manejo de información en los sistemas.

2.5. Expectativa de Daños

La expectativa de daños debe de ser la mínima, sin embargo en caso de una contingencia siempre existirá la posibilidad de que estos se presenten, por lo que a continuación se presenta una tabla con la posibilidad de ocurrencia de las amenazas consideradas.

AMENAZA	POSIBILIDAD DE OCURRENCIA
Hackeo	Baja
Virus informático	Media
Fallas en infraestructura	Media
Falla en software y equipos	Alta
Errores humanos	Media
Proveedores con fallas técnicas	Media
Errores en bases de datos	Baja
Desastres naturales	Baja

3. Medidas Preventivas

3.1. Control de Acceso

a) Acceso físico de personas no autorizadas – El acceso físico a las oficinas técnicas que se encuentran en la Empresa de Recursos Tecnológicos se encuentran restringidos, y solo personal autorizado de la misma área tendrá acceso al mismo, esto con la finalidad de evitar cualquier fallo ocasionado por personal ajeno a ésta.

Adicionalmente, el área técnica ha designado a una persona para que autorice la entrada de personal externo que requiera entrar a manipular sus propios equipos, como es el caso de los aliados estratégicos que cuentan con equipos de comunicación en las áreas de acceso restringido.

b) Acceso a la Red de Equipos y Servidores – Tanto el acceso a red de equipos y servidores, estará regulado por un controlador de dominio el cual determinará los equipos pertenecientes a la red; así como usuarios y contraseñas, brindando diferentes niveles de seguridad.

   Como medida preventiva, se solicita el cambio de la contraseña de acceso a todos los usuarios de forma periódica (cada 15 días).

c) Acceso restringido a las librerías, programas, y datos – Parte del control de usuarios por medio del controlador de dominio, es poder determinar a que tiene acceso un usuario o no, así como las capacidades de estos para instalar programas, librerías o acceso a ciertas carpetas dentro de los equipos o servidores.

3.2. Seguridad de la Información

a) Acceso remoto – El acceso remoto a los equipos o servidores de la empresa se encuentra restringido y solo personal autorizado puede hacer uso de esta herramienta.

b) Perfiles de Usuario – Según las tareas de cada usuario se crean perfiles de tal forma que la configuración del PC y el acceso a las herramientas es diferente y se adapta a las funciones de cada persona.

c) Bloqueo de Sitios WEB – Los usuarios internos navegan a través del Firewall, lo que impide la navegación a sitios WEB de contenido no apto dentro de la organización.

d) Ataque Informáticos – La empresa cuenta con filtrado y bloqueo a través del firewall lo que impide que puedan entrar a nuestra red y causarnos pérdida, sustracción o secuestro de información.

e) Seguridad Local – Por medio del Antivirus que posee la empresa se realiza bloqueo de escritura a dispositivos extraíbles con el fin de salvaguardar la información de la compañía, así como también se realiza el bloqueo de programas de almacenamiento en la nube, bloqueo de programas de conexión remota, y bloqueo de páginas con contenido de alto riesgo que puedan llegar a infectar los equipos de los usuarios y a su vez la red interna.

4. Previsión de Desastres

La previsión de desastres sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en los equipos de cómputo y comunicaciones, en la medida de que no haya situaciones que generen la interrupción del proceso de operación normal; así como el de respaldo, al tener claro los lugares de resguardo, vías de escape y de las ubicaciones de los archivos, discos con información vital de respaldo de aquellos que se encuentre aún en las instalaciones de la Empresa.

4.1. Adecuado soporte de utilitarios

Las fallas de los equipos de procesamiento de información pueden minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento.

a) Unidades de Respaldo de Energía – Este equipo deberá recibir servicios de mantenimiento preventivo al año para su correcto funcionamiento.

   El mantenimiento será realizado por la empresa contratada para realizar dicho servicio, dejando un reporte o bitácora de servicio.

b) Antenas de Comunicación – El equipo de comunicaciones punto a punto deberá de recibir servicios de mantenimiento preventivo al año, con la finalidad de asegurar su correcto funcionamiento, además de realizar ajustes en el envío y recepción de señal. El mantenimiento será dado por la empresa contratada para realizar dicho servicio, dejando un reporte o bitácora de servicio.

4.2. Seguridad Física del Personal

Como medida de seguridad física del personal, se deberán seguir las establecidas por Coordinación de Recursos Humanos y Logística de la Empresa.

4.3. Seguridad de la Información

Esta parte refiere al acceso a información contenida en los diversos sistemas de información, la cual deberá estar protegida por claves de acceso; así como un adecuado seguimiento al plan de respaldo.

4.4. Sistema de Acceso Biométrico

Sistema de Acceso Biométrico – La Empresa tiene en el Reglamento Interior de Trabajo, que el personal tiene la obligación de registrar sus entradas y salidas de las instalaciones de la empresa. Para ello la empresa tiene un sistema de acceso biométrico conocido como "Huellero Electrónico" que captura el número de identificación del empleado o la huella de éste, para así registrar la fecha y hora de entrada y salida del personal a la empresa. La responsabilidad del funcionamiento del huellero, enrolamiento de nuevos empleados y retiro de empleados que ya no laboran en la empresa es de la Subgerencia Técnica, previa notificación de la Coordinación de Recursos Humanos y Logística.

El Huellero consta de un equipo con pantalla, teclado y sensor de huella digital. La información del huellero es almacenada en una base de datos que registra el nombre, el número de identificación y la huella digital del personal, así como la configuración para cada tipo de horario y los registros de entrada y salida del personal, entre otra información.

5. Plan de Respaldo

Como parte importante de la política de continuidad se encuentra el Plan de Respaldo, el cual nos permite saber el proceso para la generación de los diferentes respaldos, ya sea de bases de datos, aplicaciones o configuraciones y nos proporcionará la medida de la pérdida de información relevante para dar continuidad a la operación de los sistemas de información Empresariales.

5.1. Respaldo de datos

a) Respaldo de Sistemas y Aplicaciones – Debido a la importancia de los sistemas y aplicaciones empresariales, es necesario realizar un proceso de respaldo que asegure que en caso de contingencia sea posible restaurar éstos para su funcionamiento. Por lo cual en este documento se explica el proceso de respaldo de los sistemas y aplicaciones.

En la empresa se manejan sistemas y aplicaciones basados en un esquema de cliente / servidor. Por lo cual los datos se respaldan independientemente de la aplicación.

- Respaldo de Datos: En la empresa todos los sistemas y aplicaciones de manejo de información cuentan con una base de datos para cada uno de ellos respectivamente.
- Respaldo del Sistema o Aplicación: Para el caso de los sistemas que se basan en clientes, basta con tener un respaldo de la última versión del código fuente e instalador.

Para el caso de los que tienen un servidor de aplicación, como las basadas en Web, es necesario respaldar constantemente la versión de producción, ya que es susceptible a modificaciones o fallos, por lo cual en caso de contingencia sería necesario restablecer la última versión funcional.

6. Plan de Recuperación

6.1. Objetivos

Los objetivos del plan de recuperación son:

- Determinación de los procedimientos para respaldar las aplicaciones y datos.
- Planificar la reactivación de la operación interrumpida producida por un desastre de los sistemas prioritarios.
- Permanente mantenimiento y supervisión de los servicios, sistemas y aplicaciones.
- Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

6.2. Alcance

El objetivo es restablecer en el menor tiempo posible el nivel de operación normal de los sitios de cómputo y telecomunicaciones, basándose en los planes de emergencia y de respaldo.

La responsabilidad sobre el Plan de Recuperación es la Dirección de Administración, la cual debe considerar la combinación de todo su personal, equipos, datos, comunicaciones y suministros.

6.3. Activación

a) Decisión – Queda a juicio de la Secretaría General determinar la activación del Plan de Contingencia.

b) Duración estimada – Dependiendo de la situación, se determinará la duración estimada de la interrupción del servicio.

c) Responsables:

- Orden de Ejecución del Plan – Secretaría General.
- Supervisión General del Plan – Coordinación de Recursos Humanos y Logística.
- Supervisión del Plan de Recuperación – Subgerencia Técnica.
- Tareas de Recuperación – Personal de tareas afines.

d) Aplicación del Plan – El plan se aplicará en caso de que se suspenda el servicio.

7. Consideraciones Adicionales

- El plan de contingencia deberá ser de conocimiento de todo la Empresa.
- La Subgerencia Técnica deberá de tener una lista de contratos y proveedores de servicios que brinden algún servicio que esté relacionado con los considerados prioritarios.
- El presente documento hace parte integral de la política general del manejo de datos personales establecido por LA EMPRESA DE RECURSOS TECNOLOGICOS, atendiendo de forma estricta los

deberes de seguridad y confidencialidad ordenados por la ley 1581 de 2012 y el decreto 1377 de 2013.

8. Anexos

8.1. Acciones de recuperación

Las acciones de recuperación serán diseñadas para cada uno de los impactos mostrados anteriormente, definiendo asimismo los responsables de dichas actividades.

a) Falla en comunicación a Internet.

ACCIONES	RESPONSABILIDAD
Verificar el equipo (Firewall).	Subgerencia Técnica
Verificar Router de frontera.	Subgerencia Técnica
Verificar estado de alarmas en los equipos de enlace a Internet del proveedor. En caso de alarmas levantar reporte con el proveedor. Dar seguimiento con el proveedor de servicio de internet.	Subgerencia Técnica

b) Falla en comunicación entre inmuebles

ACCIONES	RESPONSABILIDAD
Verificar los equipos de interconexión del enlace entre inmuebles.	Subgerencia Técnica
Verificar el estado de la fibra óptica o los enlaces de respaldo por radio enlace.	Subgerencia Técnica

c) Falla en comunicación de voz

ACCIONES	RESPONSABILIDAD
Verificar si la central telefónica está alarmada, y en caso de ser necesario llamar al proveedor de telefonía.	Subgerencia Técnica
Identificar si la falla es interna y corresponde a ERT la solución de la misma.	Subgerencia Técnica

d) Falla en el suministro de Energía

ACCIONES	RESPONSABILIDAD
Verificar que la unidad de respaldo de energía entre en operación.	Subgerencia Técnica

Verificar tiempo de respaldo y consultarlo continuamente.	Subgerencia Técnica
Informar a los usuarios que apaguen los equipos a su cargo.	Subgerencia Técnica
Al faltar 5 minutos para agotarse la energía, apagar los servidores.	Subgerencia Técnica
Al agotarse la energía, verificar que las baterías internas de los equipos que las posean, entren en operación.	Subgerencia Técnica
Poner en bypass la unidad de respaldo si la falla obedece estrictamente a esta, y de esta forma tomar la energía eléctrica de forma directa, al tiempo que se corrige el problema.	Subgerencia Técnica

e) Falla en el hardware y/o software de los servidores

ACCIONES	RESPONSABILIDAD
En caso de falla del disco duro, reemplazarlo; en caso de falla de algún otro componente o en el sistema operativo realizar cambio de servidor al tiempo que se realiza mantenimiento correctivo al equipo afectado.	Subgerencia Técnica

f) Falla en aplicaciones

ACCIONES	RESPONSABILIDAD
Si se reporta pérdida de información en las bases de datos, restablecer el último respaldo realizado.	Subgerencia Técnica

g) Virus Informático

ACCIONES	RESPONSABILIDAD
La información contenida en los equipos de cómputo de cada usuario interno es responsabilidad de cada uno de ellos, y por tanto el área de servicios telemáticos no se hace responsable por pérdida de información en los equipos de los usuarios.	Subgerencia Técnica
En caso de detectar un virus informático que sature la red, se realizará monitoreo a la red para localizar el origen del tráfico excesivo y eliminar la causa del problema.	Subgerencia Técnica
En caso de verse afectado algún equipo en el hardware o software debido a un virus, se realizará el respectivo mantenimiento correctivo.	Subgerencia Técnica

9. Responsable del Documento

Subgerencia Técnica

Última Modificación: 07/01/2022

Tel: (572) 620-2020 | ertcali@ert.com.co
Av. 2BN No. 23N-47, Edificio Estación del Ferrocarril
Piso 2, Cali - Colombia www.ert.com.co