PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA CONTRALORIA GENERAL DEL DEPARTAMENTO DEL CHOCO

CONTRALORÍA
General Departamento del Chocó

INTRODUCCION

La Contraloría General del Departamento del Chocó considera que la información en una entidad es el bien más importante, por este motivo debemos protegerla ante la posible pérdida, destrucción, robo y otras amenazas, con la preparación e implementación de este Plan.

La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información para el funcionamiento de la Entidad y están expuestos a diversos Factores de Riesgos Humanos y Físicos.

El Plan de tratamiento de Riesgo de seguridad y privatización de la información, está encaminado a establecer y evaluar las posibles acciones para mitigar los riesgos existentes.

El Plan busca evaluar, mantener y mejorar los procedimientos de recuperación, que permitan mitigar los daños potenciales antes que un “desastre” ocurra; y además facilitar la recuperación en el evento de un desastre.

La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

- **Crítica**: Es indispensable para la operación de la empresa.
- **Valiosa**: Es un activo de la empresa y muy valioso.
- **Sensible**: Debe de ser conocida por las personas autorizadas

DEFINICIONES

- **Riesgo**: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.

- **Amenaza**: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un prejuicio o impacto negativo en la institución.

- **Vulnerabilidad**: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- **Impacto**: son las consecuencias que genera un riesgo una vez se materialice.

- **Seguridad**: Es una forma de protección contra los riesgos. La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

OBJETIVOS

- Planear y ejecutar las tareas para proteger la Información contra los daños que se pueden producir por los fenómenos naturales, cortes de energía y/o por manos inescrupulosas.

- Clasificar la Información de acuerdo a su importancia y su reserva.

- Garantizar la continuidad de las principales operaciones que componen los Sistemas de Información.

- Implementar actividades que permitan evaluar y retroalimentar el Plan una vez se obtengan los resultados.

Bienes y Servicios Susceptibles de Daños

- Software.
- Contabilidad.
- Sitio Web

Principales servicios que deberán ser restablecidos Y/O recuperados

- Windows.
- Correo Electrónico.
- Internet.
- Antivirus.
- Herramientas de Microsoft Office.
- Base de Datos Confianza (software financiero)
- Backup de la Información.

Respaldo de la Información

- Backup de la Base de Datos Confianza
- Backup del sitio WEB
- Backup del Servidor.

ANALISIS DE RIESGOS

1. Bienes susceptibles de daño

- Personal
- Hardware
- Software y utilitarios
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones

2. Daños

- Dificultad de acceso a los recursos por problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.
- Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales.
- Divulgación de información a instancias fuera de la Entidad y que afecte su patrimonio, sea mediante Robo o Infidencia.

3. Fuentes de daño

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistema computacionales
- Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente o la red de energía eléctrica).
- Fallas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo y Otros).
- Fallas de Hardware (Equipos de Cómputo, Servidores o Red Switches, cableado de la Red, Router, FireWall).

CLASES DE RIESGOS

- Incendio o Fuego
- Falla en los equipos de computo
- Acción virus informático
- Fenómenos naturales
- Accesos no autorizados y divulgación de la información
- Ausencia del personal de sistemas.

MINIMIZACION DEL RIESGO

Teniendo en cuenta lo anterior, corresponde al presente Plan de Contingencia y de seguridad y privatización de la información, minimizar estos índices con medidas preventivas y correctivas sobre cada uno de los Riesgos.

Es de tener en cuenta que en lo que respecta a Fenómenos naturales, en esta región se han registrado en estos últimos tiempos movimientos telúricos de muy poca intensidad; sin embargo, las lluvias fuertes y tormentas eléctricas producen mayores estragos, originando filtraciones de agua en los edificios, produciendo cortes de luz, cortos circuitos.

Riesgo	Grado	Frecuencia	Acción	Observaciones
Incendio o Fuego	Moderado	Aleatorio	Extintor	Hay un solo extintor para todas las oficinas, realizar backup
Falla en los Equipos	Alto	Aleatorio	Realizar mantenimiento preventivos y/o correctivos, conectarlos a UPS	Problemas con las UPS, se encuentran en mal estado
Acción virus informático	Moderado	Continuo	Antivirus actualizado	Se debe evitar que las licencias de antivirus expiren, se requiere renovación con anterioridad del nuevo antivirus
Fenómenos naturales	Grave	Aleatorio	Ubicar los equipos estratégicamente, protegiéndolos en caso de lluvias o terremotos	Realizar mantenimientos periódicos a las instalaciones de la CGCH
Accesos no autorizados y divulgación de la información	Grave	Aleatorio	Asignación de usuarios y claves, mantener reserva en la información.	El usuario y la contraseña es personal y no se debe entregar a terceras personas, que los funcionarios no

				divulguen información de reserva.
Ausencia del personal de sistemas	Moderado	Aleatorio	Capacitar a otro funcionario o un pasante en caso de las ausencias del administrador de sistemas	Solo se cuenta con una persona en el área de sistemas.

- Incendio o Fuego

a. Realizar capacitación para el manejo de extintores y primeros auxilios.
b. El servidor realiza backups de la información diariamente.
c. Realizar backups del servidor de forma mensual, almacenada en DVD y ubicarlos estratégicamente cerca a la salida principal de la Entidad.

- Falla en los Equipos

a. Realizar mantenimiento preventivo y/o correctivo de equipos por lo menos dos veces al año y a su vez a la red de voz y datos, a su vez falta la instalación de una UPS general que soporte todos los equipos.
b. Realizar backup de los archivos en l servidor y en medios externos, se debe ubicar en un lugar segura cerca a la salida del edificio.

- Acción de Virus Informático

a. Se cuenta con un software antivirus para la entidad, pero su actualización no se realiza de forma inmediata a su expiración. Se requiere renovación con anterioridad del nuevo antivirus.
b. Únicamente es el administrador de la red es el encargado de cambiar configuraciones y tiene acceso al servidor.

- Fenómenos Naturales

a. No han ocurrido fenómenos naturales como terremotos o inundaciones en los últimos años, y la probabilidad de ocurrencia es baja, de igual forma hay que contar con algunas medidas de prevención.

- Accesos No Autorizados y divulgación de la información reservada

a. Se controla el acceso al sistema de red mediante la definición de un administrador con su respectiva clave.
b. Clasificar la información de acuerdo a su reserva y su importancia y a su vez capacitar a los funcionarios sobre la no divulgación de la misma.

- Ausencia del personal de sistemas

a. En la Contraloría General del Departamento del Chocó, solo cuenta con un funcionario en al aérea de Sistemas; es la única persona con claves de acceso al sistema, que conoce del manejo de la red y los sistemas de información.

RIESGO EVENTO

- Fallas Tarjeta de Red.
- Fallas Punto de Swicht.
- Fallas Punto Pacht Panel.
- Fallas Punto de Red.

NO EXISTE COMUNICACIÓN ENTRE CLIENTE Y SERVIDOR

- Fallas de Componentes de Hardware del Servidor.
- Falla del UPS (Falta de Suministro eléctrico).
- Virus.
- Sobrepasar el límite de almacenamiento del Disco

FALLAS EN EL EQUIPO SERVIDOR

- Daños por refrigeración
- Pérdida de Información

AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE SISTEMAS.

- Incapacidad
- Accidente
- Renuncia Intempestiva

INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.

- Falla de equipos de comunicación: SWITCH

- Falla en los equipos de cómputo.
- Fallas en el software de Acceso a Internet.
- Perdida de comunicación con proveedores de Internet.

PERDIDA DE SERVICIO DE INTERNET

- Sabotaje
- Daño en el Router
- Terremoto

CONTINGENCIA

FALLA DEL SERVIDOR

1. Daño Disco duro
2. No arranca el servidor, no es posible ingresar
3. Hace un ruido extraño

Recursos de Contingencia

a. Ubicar el disco malo.
b. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
c. Bajar el sistema y apagar el equipo.
d. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
e. Restaurar el último backup en el disco.
f. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
g. Habilitar las entradas al sistema para los usuarios.

FALLA EN LOS EQUIPOS DE CÓMPUTO

1. Daños de Hardware.
2. Daños en el Software
3. Daño Carpetas o archivos

Recursos de Contingencia

a. Componente de Remplazo (Memoria, Disco Duro, etc.).
b. Software licenciado
c. Backup diario de información de los archivos en medios físicos y en el servidor

AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE LA UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN

1. Directriz del contralor (escrita o Email) contratar o buscar pasante que se encargue del área de sistemas en la CGCH, especificando el periodo de asignación.

2. Obtener la relación de los Sistemas de Información con los que cuenta la CGCH, detallando usuarios, en que equipos se encuentran instalados y su utilidad.

3. Conocer la ubicación de los backups de información.

Recursos de Contingencia

a. Relación de los sistemas de información de la CGCH.
b. Mapa de la Red de la CGCH actualizado.
c. Relación de las IP

INTERRUPCIÓN DEL FLUIDO ELÉCTRICO EN EL HORARIO LABORAL

1. La UPS mantendrá activo los servidores y los PC, mientras se repare la energía eléctrica.

2. Para el caso de apagón se mantendrá la autonomía de corriente que la UPS brinda.

Recursos de contingencia

a. Adquirir una UPS que soporte todos los equipos de cómputo, el servidor y el RAD de comunicaciones.

PERDIDA DE SERVICIO INTERNET

1. Realizar pruebas para identificar posible problema dentro de la entidad
2. Si se evidencia problema en el hardware, se procederá a cambiar el componente
3. Si se evidencia problema con el software, se debe reinstalar el sistema operativo del servidor
4. Si no se evidencia falla en los equipos de la entidad, se procederá a comunicarse con la Empresa prestadora del servicio, para asistencia técnica.
5. Es necesario registrar el daño para llevar un historial que servirá de guía para futuros daños.
6. Verificar el pago oportuno del servicio.

Recursos de Contingencia

a. Hardware
b. Router
c. Software
d. Herramientas de Internet.

CONCLUSIONES

En la informática, un plan de contingencia es un programa alternativo para que una Entidad pueda recuperarse de un desastre informático y restablecer sus operaciones con rapidez y este depende de la infraestructura y las funciones que se realizan en el área de sistemas.

El Plan de contingencias y Seguridad en Información de la Contraloría General del Departamento del Chocó, busca que el bien más importante de la Entidad como es la Información permanezca a salvo así como salvaguardar la infraestructura de la Red, los Sistemas de Información y el buen funcionamiento tanto del servidor como de los equipos de cómputo.

Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de riesgos, Minimización de riesgos, Identificación de posibles eventos para el Plan de Contingencia, Establecimiento del Plan de Recuperación y Respaldo, Plan de Emergencias y Verificación e implementación del plan.

CONTRALORÍA
General Departamento del Chocó

RECOMENDACIONES

Dar a conocer el contenido de este Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información a todo el personal de la Contraloría General del Departamento del Chocó, igualmente se deben desarrollar las acciones correctivas para minimizar los riegos identificados.

Capacitar un funcionario con la información mínima para que no se vayan a ver afectado el normal funcionamiento de la entidad, para el caso en que el funcionario del área de sistemas se encuentre ausente.

Atentamente,

TATIANA VALENCIA ASPRILLA
Contralora General del Departamento del Chocó

Proyecto: Rosa Diaz – Profesional Universitario