SUPERINTENDENCIA DE ORDENAMIENTO TERRITORIAL, USO Y GESTIÓN DEL SUELO

Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales - CGDIG

Plan de Contingencia de Tecnologías de la Información y Comunicaciones de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo

2018 - 2022

Control del Documento				
Elaborado por:	**Cargo**	**Versión:**	**Fecha:**	**Firma**
Ing. Mónica Uyana García	Coordinadora General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG)	1.0	30 de abril de 2018	
Actualizado por:	**Cargo**	**Versión:**	**Fecha:**	
Ing. Mónica Uyana García	Coordinadora General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG)	1.1	03 de julio de 2018	
Aprobado por:	**Cargo**	**Versión:**	**Fecha:**	
Arq. Fernando Pauta Calle	Superintendente de Ordenamiento Territorial, Uso y Gestión del Suelo (Subrogante)	1.1	06 de julio de 2018	

Contenido

PLAN DE CONTINGENCIA

PRESENTACIÓN

El Plan de Contingencia Informático implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Es responsabilidad de todas las unidades que conforman la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo (SOT) aplicar todas las medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

El alcance de este plan guarda relación con la infraestructura informática, así como los procedimientos relevantes asociados con la plataforma tecnológica. La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función del negocio. Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que el personal realiza frecuentemente al interactuar con la plataforma informática (entrada de datos, generación de reportes, consultas, etc.).

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. La información como uno de los activos más importantes de la Superintendencia, es el fundamento más importante de este Plan de Contingencia.

Al existir siempre la posibilidad de desastre, pese a todas nuestras medidas de seguridad, es necesario que el Plan de Contingencia Informático incluya el Plan de Recuperación de Desastres con el único objetivo de restaurar el Servicio Informático en forma rápida, eficiente, con el menor costo y perdidas posibles.

La protección de la información es vital ante la posible pérdida, destrucción, robo y otras amenazas que puede afronta una institución, razón por la cual es importante la preparación e implementación de un Plan de Contingencia Informático.

El plan de Contingencia indica las acciones que deben tomarse inmediatamente tras el desastre. Un primer aspecto importante del plan es la organización de la contingencia, en el que se detallan los nombres de los responsables de la contingencia y sus responsabilidades. El segundo aspecto crítico de un Plan de Contingencia es la preparación de un Plan de BackUp, elemento primordial y necesario para la recuperación. El tercer aspecto es la preparación de un Plan de Recuperación. La empresa debe establecer su capacidad real para recuperar información crítica en un periodo de tiempo aceptable.

Otro aspecto importante del plan de recuperación es identificar el equipo de recuperación, los nombres, números de teléfono, asignaciones específicas, necesidades de formación y otra información esencial, para cada miembro del equipo que participa en el Plan de recuperación.

La base del Plan de Contingencia y su posterior recuperación, es establecer prioridades claras sobre qué tipo de procesos son los más esenciales. Es necesario por tanto la identificación previa cuales de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión.

El plan de contingencia informático, debe contemplar los planes de emergencia, BackUp, recuperación, comprobación mediante simulaciones y mantenimiento del mismo. El Plan de Contingencia debe brindar el apoyo necesario para la recuperación rápida del control y capacidades para procesar la información y restablecer la marcha normal de la institución, mismo que debe ser revisado de manera permanente para su actualización y modificación, considerando las actualizaciones e innovación tecnológica habilitada y disponible en la institución para la mitigación de riesgos y control de incidentes de seguridad tecnológicos, ambientales, y de la información.

1. ANÁLISIS DE SITUACIÓN TECNOLÓGICA

Propósito:

Cualquier Sistema de Redes de Computadoras (CPU, periféricos y accesorios) está expuesto a riesgos y pueden ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos.

Frente a cualquier evento, la celeridad en la determinación de la gravedad del problema depende de la capacidad y la estrategia a seguir para señalar con precisión, por ejemplo: ¿Qué componente ha fallado? ¿Cuál es el dato o archivo con información que se ha perdido, ¿En que día y hora se ha producido? y ¿Cuán rápido se descubrió el incidente? Estos problemas sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información asociados al Plan de Contingencia.

Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (discos duros, servidores, procesadores, storage, entre otros), sea por desastres (incendios, terremotos, sabotaje, entre otros) o por fallas técnicas (errores humanos, virus informático, entre otros), que pueden producir un daño físico irreparable. Frente al mayor de los desastres solo queda el tiempo de recuperación, lo que significa adicionalmente la fuerte inversión en recursos humanos y técnicos para reconstruir su Sistema de Red y su Sistema de Información.

Objetivo:

- Garantizar la continuidad de las operaciones de los Sistemas de Información vitales para la operación de la Institución.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información vital para la operación de la Institución.

Importancia:

- Garantizar la seguridad física de las personas, la integridad de los activos lógicos y materiales de los sistemas de información de datos vitales para la operación de la institución.
- Permitir realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que en él se puedan derivar.
- Permitir realizar un Análisis de Riesgos, Respaldo de los datos y su posterior Recuperación de los datos. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de la Institución. La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la Institución.
- Permitir definir contratos de seguros, que vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades.

2. ANÁLISIS DEL SISTEMA DE RED DE DATOS

La Administración de Red está dividida en dos clases:

a) Conectividad: se encargada de la conexión alámbrica e inalámbrica de los equipos de computación

b) Manejo de servidores: se encarga de alojar todos los servicios y sistemas de comunicación e información.

- Servidor de Correo Electrónico
- Servidor de Directorio Activo
- Servidor Proxy Reverso NGINXS
- Servidor de Almacenamiento en la Nube Institucional (SOTCloud)
- Servidor de Gestión de Tickets y Mesa de Servicios (OTRS)
- Servidor web para la operación de la Intranet Institucional
- Servidor web para la operación del Sistema de Información Territorial (SIT)
- Servidor web para la operación de la aplicación móvil MiTierra
- Servidor web para la operación del Sistema Integral Cero Papeles (SISOT)
- Servidor para alojamiento del FME Server (procesamiento de datos geoespaciales)
- Servidor web para el manejo de geoportales GEODB
- Servidor web para el manejo de geoportales GEOToolBox

c) Sistemas de Información

El Sistema de Información, incluye la totalidad del Software de Aplicación, Software en Desarrollo, conjunto de Documentos Electrónicos, Bases de Datos e Información Histórica registrada en medios magnéticos e impresos en papeles, Documentación y Bibliografía.

3. PLAN DE REDUCCIÓN DE RIESGOS

El Plan de Reducción de Riesgos es el equivalente a un Plan de Seguridad, en el que se consideran todos los riesgos conocidos, para lo cual se debe efectuar un Análisis de Riesgos.

3.1 Análisis de Riesgos

Es importante realiza el análisis de riesgo a todos los equipos y sistemas informáticos que alojan información vital para la Institución, con el objeto que sean protegidos.

3.1.1 Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

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

3.1.2 Daños

Los posibles daños pueden referirse a:

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, desastres naturales o fallas humanas.
- Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.
- Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

3.1.3 Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la institución son:

- 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, la red de energía eléctrica, no acondicionamiento atmosférico necesario).

- Fallas de Personal Clave, por los siguientes inconvenientes:
  - Enfermedad
  - Accidentes
  - Renuncias
  - Abandono de sus puestos de trabajo, Otros.

- Fallas de Hardware:
  - Falla en los Servidores (Hardware)
  - Falla en el hardware de Red (Switches, cableado de la Red, Router, Firewall)

- Incendios:
  - Falla en los equipos de detección y prevención de incendios
  - Extintores de incendios caducados o inservibles.

3.1.4 Características

El Análisis de Riesgos tiene las siguientes características:

- Es posible calcular la probabilidad de que ocurran las cosas negativas.
- Se puede evaluar económicamente el impacto de eventos negativos.
- Se puede contrastar el Costo de Protección de la Informática y medios versus el Costo de volverla a producir.

Durante el estudio Análisis de Riesgo, se define claramente:

- Lo que intentamos proteger
- El valor relativo para la organización
- Los posibles eventos negativos que atentarían lo que intentamos proteger.
- La probabilidad de ataque.

Se debe tener en cuenta la probabilidad de suceso de los problemas posibles, de tal manera que sea posible realizar la tabulación del problema asociado a un costo. Los criterios que usaremos para tipificar los posibles problemas son:

Criterios	Escala			
Grado de Negatividad	Leve	Moderado	Grave	Muy severo
Posible Frecuencia del Evento negativo	Nunca	Aleatorio	Periódico	Continuo

Criterios	Escala			
Grado de impacto o consecuencias	Leve	Moderado	Grave	Muy severo
Grado de Certidumbre	Nunca	Aleatorio	Probable	Seguro

Tabla: Escala de Valores para Criterios de Posibles Problemas

3.1.5 Clases de Riesgo

La tabla proporciona el Factor de Probabilidad por Clase de Riesgo en función a la ubicación geográfica de la institución y a su entorno institucional, por ejemplo:

- La institución se encuentra ubica en una zona sísmica el factor de probabilidad de desastre por terremotos será alta.
- La institución, se ubica en una zona marginal con alto índice de delincuencia, las probabilidades de robo, asalto o vandalismo será de un sesgo considerablemente alto.
- La institución se ubica en una zona industrial las probabilidades de "Fallas en los equipos" será alto por la magnitud de variaciones en tensiones eléctricas que se generan en la zona.
- En la institución se cambia constantemente de personal, las probabilidades de equivocaciones y sabotaje será alto

3.2 Identificación de Amenazas:

Escala Factor de Probabilidad por Clase de Riesgo

Clase	Factor
Incendio o Fuego	0.40
Robo común de equipos y archivos	0.75
Sabotaje	0.60
Falla en los equipos	0.40
Equivocaciones	0.70
Acción virus informático	0.50
Fenómenos naturales	0.25
Accesos no autorizados	0.75
Robo de datos	0.80
Manipulación y sabotaje	0.80

Tabla: Factores de probabilidad por clase de riesgo

En lo que respecta a fenómenos naturales, nuestra región ha registrado en estos últimos tiempos movimientos telúricos de intensidad media y alta; sin embargo, las lluvias fuertes producen mayores estragos, originando filtraciones de agua en los edificios de techos, produciendo cortes de luz, cortos circuitos (que podrían desencadenar en incendios).

3.2.1 INCIDENTE 1 Clase de Riesgo: Incendio o Fuego

Grado de Negatividad: Muy
Severo Frecuencia de Evento: Aleatorio
Aleatorio Grado de Impacto: Grave
Grado de Certidumbre: Probable

Situación actual	Acción correctiva
El Data Center de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo no cuenta con un Sistema de detección y mitigación de incendios	Se requiere la implementación de un sistema de detección y prevención de incendios .

Tabla: Incendio o Fuego

Una probabilidad máxima de contingencia de este tipo en la institución, puede alcanzar a destruir un 50% de las oficinas antes de lograr controlarlo, también podemos suponer que en el área de Servidores tendría un impacto mínimo, por las medidas de seguridad y ambiente que lo protege. Esta información permite resaltar el tema sobre el lugar donde almacenar los BackUp.

El incendio, a través de su acción calorífica, es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD, DVD, cartuchos, Discos duros, las mismas que residirán en una caja fuerte como medio de seguridad que protegerá la información frente a intentos de robo, desastres naturales, pero no del calor. Estos dispositivos de almacenamiento muestran una tolerancia de temperatura de 5°C a 45°C, y una humedad relativa de 20% a 80%.

Para la mejor protección de los dispositivos de almacenamiento, se colocarán estratégicamente en lugares distantes, con una Segunda Copia de Seguridad custodiada en un lugar externo de la oficina matriz de la SOT.

En las áreas funcionales distribuidas, existen varios equipos tecnológicos tales como portátiles, equipos de escritorio, impresoras, proyectores, dispositivos inalámbricos, access point, entre otros que pueden reaccionar al calor y producir un incremento del nivel del incendio, razón por la cual se require incluir elementos y medidas de seguridad contra incendios.

Se requiere principalmente la habilitación de un Sistema de control de incendios, para la prevención de incendios, así como extintores para contrarrestar el incendio. Su uso conlleva a colocarlos cerca de las posibles áreas en las que se puede materializar un incendio.

Acciones a considerer contra Daños por Incendios:

- Cuando el daño del edificio ha sido mayor, evaluar el traslado a un nuevo local, hasta considerar la posibilidad del traslado.

- Cuando el daño ha sido menor:

  - Tramitar la garantía de los equipos dañados o comprar los equipos indispensables para la continuidad de las operaciones. Responsable Dirección Administrativa de la Coordinación General Administrativa Financiera (CGAF).

  - Se recopilan los respaldos de datos, programas, manuales y claves. Responsable encargado de Infraestructura de la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG).

  - Instalar el sistema operativo. Responsable encargado de Soporte y Mantenimiento Infraestructura Tecnológica de la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG).

  - Restaurar la información de las bases de datos y programas de los Sistemas de Información indispensables para la operación de la Institución. Responsable encargado de Desarrollo de Software de la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG).

  - Revisar y probar la integridad de los datos. Responsable encargado de Desarrollo de Software de la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG).

ACCIONES A TOMAR ANTES:

- Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado.
- No concentrar grandes cantidades de papel junto a equipos que generen calor, ni fumar cerca de químicos o sustancias volátiles.
- Verificar las condiciones de extintores e hidratantes y capacitar para su manejo.
- No fumar dentro de las oficinas para evitar la activación de los sensores de humo, así como cualquier probabilidad de incendio.
- En los lugares autorizados para fumar, procurar no arrojar las colillas a los cestos de basura, verificar que se hayan apagado bien los cigarrillos y no dejarlos en cualquier sitio, utilizar ceniceros.
- No almacenar sustancias y productos inflamables.
- No realizar demasiadas conexiones en contactos múltiples, evitar la sobrecarga de circuitos eléctricos.
- Por ningún motivo se deben mojar las instalaciones eléctricas, recordar que el agua es un buen Conductor de la electricidad.
- Si se detecta cualquier anomalía en los equipos de seguridad (extintores, hidratantes, equipo de protección personal, etc.) y en las instalaciones eléctricas, reportar de inmediato a Seguridad.
- Mantener siempre el área de trabajo limpia y en orden, ya que no hacerlo es una de las causas que provocan incendios.

- Tener a la mano los números telefónicos de emergencia.
- Portar siempre la credencial de identificación de la SOT.

DURANTE:

- Ante todo se recomienda conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá (si el tiempo lo permite) "Salir de Red y Apagar Computador": Down en el (los) servidor(es), apagar (OFF) en la caja principal de corriente que alimenta al Data Center.
- Si se conoce sobre el manejo de extintores, intenta sofocar el fuego, si este es considerable no trates de extinguirlo con los propios medios, solicitar ayuda.
- Si el fuego está fuera de control, realizar evacuación del inmueble, siguiendo las indicaciones del personal de bomberos.
- No utilizar elevadores, descender por las escaleras pegado a la pared que es donde posee mayor resistencia, recuerda: No gritar, No empujar, No correr y dirigirse a la zona de seguridad.

DESPUÉS:

- Retirarse inmediatamente del área incendiada y ubícarse en la zona de seguridad externa que corresponda.
- No obstruir las labores del personal especializado, dejar que los profesionales se encarguen de sofocar el incendio.
- El personal calificado realizará una verificación física del inmueble y definirá si esa en condiciones de ser utilizado normalmente.
- Colaborar con las autoridades.

3.2.2 INCIDENTE 2 Clase de Riesgo: Robo Común de Equipos y Archivos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Moderado Grado de
Certidumbre: Aleatorio

Situación actual	Acción correctiva
No existe vigilancia permanente.	La SOT debe contratar personal de seguridad para la institución.
No se verifica si el Personal de Seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada.	Se debe efectuar la contratación de personal de seguridad para la SOT.

La Unidad de Bienes sigue un proceso empírico para la asignación y retiro de equipos informáticos	Se debe establecer un proceso formal para la entrega y retiro de equipos informáticos.

Tabla: Robo Común de Equipos y Archivos

Se han reportado casos en los cuales ha existido manipulación y reubicación de equipos sin el debido conocimiento y autorización debida en la Unidad de Bienes.

Acciones a tomar:

Analizar las siguientes situaciones:

- En qué tipo de vecindario se encuentra la Institución.
- Personal externo puede fácilmente accede a los equipos tecnológicos de la institución sin ser detectado.
- Hay personal de seguridad que vigila las entradas y salidas del edificio, pero no existen cámaras de monitoreo o de videovigilancia que permitan identificar actividades sospechas o posibles personas que comentan actos de robo en la institución.
- Cuánto valor tienen actualmente las Bases de Datos.
- Cuánta pérdida podría causar en caso de que se hicieran públicas.
- Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.
- Trabajo no supervisado, especialmente durante el turno de noche, malas técnicas de contratación, evaluación y de despido de personal.

3.2.3 INCIDENTE 3 Clase de Riesgo Vandalismo

Clase de Riesgo: Vandalismo

Grado de Negatividad: Moderado
Frecuencia de Evento: Aleatorio
Aleatorio Grado de Impacto: Grave
Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo, está en una zona donde el índice de vandalismo es bajo	Se debe realizar la contratación de personal de vigilancia.

Situación actual	Acción correctiva
Se presentan casos muy aislados de personas que no están conformes con algunas normativas administrativas, y al efectuar los reclamos las personas asumen actitudes retroactivas, que muchas veces ofenden al trabajador, y sin medir las consecuencias pueden llegar a agreder al personal de la Institución así como a alguna instalación de la Superintendencia.	Se debe realizar la contratación de personal de vigilancia, e implementar cámaras de videovigilancia.
Alguna probabilidad de disturbios por manifestaciones políticas.	Se debe realizar la contratación de personal de vigilancia.

Tabla: Riesgo o Vandalismo

La destrucción del equipo puede darse por una serie de desastres incluyendo el vandalismo, robo y saqueo en simultáneo.

Acciones a tomar

- Si el intento de vandalismo es mayor, se presenta un grave riesgo dentro del área del Centro de Cómputo ya que puede dañar los dispositivos perdiendo toda la información y por consecuencia las actividades se verían afectadas en su totalidad, así como el servicio proporcionado.

A continuación se menciona una serie de medidas preventivas:

- Establecer vigilancia mediante cámaras de seguridad en el sitio, el cual registre todos los movimientos de entrada del personal.
- Instalar identificadores mediante tarjetas de acceso o lectores de huella.
- Determinar lugares especiales, fuera del centro de datos, para almacenar los medios magnéticos de respaldo y copia de la documentación de referencia y procedimientos de respaldo y recuperación (se puede contratar una caja de seguridad externa donde se custodiaran los datos e información crítica).

Los principales conflictos que pudieran presentarse son:

- En cuanto a la red, si el sistema llegará a presentar una falla no habría personal que atendiera la problemática y por consecuencia se detendrían las operaciones a falta del monitoreo a los distintos sistemas.

- Respecto a los dispositivos de almacenamiento, si se mantienen los respaldos únicamente dentro de la Institución sería imposible reanudar las actividades que un momento dado fueran críticas, como el Sistema Integral SISOT, Sistema de Información Territorial SNIT, la nómina, contabilidad, etc.; en un sitio alterno, ya que no contarían con copia de la información.

3.2.4 INCIDENTE 4 Clase de Riesgo: Falla de Equipos

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Aleatorio Grado de Impacto: Grave
Grado de Certidumbre: Probable

Situación actual	Acción correctiva
La Superintendencia cuenta con una Red Eléctrica estabilizada, sin embargo no en todas las Intendencias Zonales se cuenta con el servicio de energía eléctrica estable.	Proponer un Estudio para instalar una Red Eléctrica Estabilizada.
Se desconoce la existencia de un adecuado tendido eléctrico para las nuevas oficinas zonales de la SOT para ser habilitadas en el 2do trimestre del año 2018 y siguientes años.	Tomar previsiones económicas para implementar un adecuado tendido eléctrico.
Cada área funcional se une a la Red a través de gabinetes, la falta de energía en éstos, origina la ausencia de uso de los servicios de red, comunicaciones, Sistemas Informáticos, videoconferencia, entre otros.	Proteger los gabinetes, y su adecuado apagado y encendido, dependen los servicios de red en el Área.
La inoperatividad de los equipos tecnológicos, requiere un rápido mantenimiento o reemplazo.	Los equipos tecnológicos de la SOT cuentan con garantía por 3 años. Los repuestos y partes de cambio serán efectuadas por el mismo proveedor conforme cronograma de mantenimiento de equipos tecnológicos.

Tabla: Falla de equipos

De ocurrir esta contingencia las operaciones informáticas se detendrían, puesto que los dispositivos en los que se trabaja dependen de la corriente eléctrica para su desempeño. Si el corte eléctrico dura poco tiempo las operaciones no se ven afectadas gravemente, pero si el corte se prolongara por tiempo indefinido provocaría un trastorno en las operaciones del día, sin afectar los datos.

El equipo de aire acondicionado y ambiente adecuado en el Área de Servidores, favorece su correcto funcionamiento.

Para el adecuado funcionamiento de las computadoras personales, necesitan de una fuente de alimentación eléctrica fiable, es decir, dentro de los parámetros correspondientes. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa (fuera de los valores normales), las consecuencias pueden ser muy serias, tal como daño del HW y la información podría perderse.

La fuente de alimentación es un componente vital de los equipos de cómputo, y soportan la mayor parte de las anomalías del suministro eléctrico. Se ha identificado los siguientes problemas de energía más frecuentes:

- Fallas de energía.
- Transistores y pulsos.
- Bajo voltaje.
- Ruido electromagnético.
- Distorsión.
- Variación de frecuencia.

Para los cuales existen los siguientes dispositivos que protegen los equipos de estas anomalías:

- Supresores de picos.
- Estabilizadores.
- Sistemas de alimentación ininterrumpida (UPS).

Existen formas de prever estas fallas, con la finalidad de minimizar su impacto, entre ellas tenemos:

Tomas a Tierra o Puestas a Tierra:

Se denomina así a la comunicación entre el circuito Eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una rotura del aislamiento eléctrico. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en tierra humedad, con o sin agregados de ciertos componentes de carbón vegetal, sal o elementos químicos, según especificaciones técnicas indicadas para las instalaciones eléctricas.

En la práctica protege de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y para disipar sobretensiones de origen atmosférico o industrial.

La Toma a Tierra tiene las siguientes funciones principales:

a) Protege a las personas limitando la tensión que respecto a tierra puedan alcanzar las masas metálicas.
b) Protege a las personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.
c) Facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico.

Las inspecciones deben ser realizadas trimestralmente, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se realice en los meses de verano o en tiempo de sequía. Es recomendable un mantenimiento preventivo anual dependiendo de las propiedades electroquímicas estables.

Fusibles:

Al cablear la computadora, la carcasa normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad se fugara a través del aislante y llegase a la carcasa, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito.

Este incremento puede ser detectado por un fusible o un diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecarga (un fusible se debe sustituir tras fundirse, un diferencial se debe restaurar tras saltar).

Si una parte de una computadora funde un fusible o hace saltar un diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema se puede a conectar el equipo.

Al sustituir los fusibles de una computadora, se debe tener cuidado que todos los equipos estén apagados y desconectados antes de cambiar el fusible. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado.

Asegurarse que el fusible de recambio es de la misma capacidad que el fundido.

Por ejemplo si el fusible fundido viene marcando 2 amperios, no se debe sustituir por uno de 3 amperios. Un fusible de 3 amperios dejara pasar 1 amperio más de la intensidad de lo que fijo el diseñador del equipo.

Extensiones eléctricas y capacidades:

Las computadoras ocupan rápidamente toda la toma de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado.

No solo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. A parte del daño físico que puede provocar engancharse repentinamente con el cable, apaga de forma rápida un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.
- Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.
- No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar.
- Se deben utilizar los enchufes de pared siempre que sea posible.
- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o

diferenciales. Esto puede ayudar limitar el daño ante fallas eléctricas.

- Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esa cifra el amperaje total de todos los aparatos conectados a ella.
- Adquirir toma de corrientes de pared o extensiones eléctricas mixtas, capaces de trabajar con enchufes de espigas planas, como cilíndricas.
- Tanto las tomas corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

Error Físico de Disco de un Servidor (Sin RAID):

Dado el caso crítico de que el disco presenta fallas, que no puedan ser reparadas, se deben considerer las siguientes acciones:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último BackUp, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Verificación el buen estado de los sistemas.
8. Habilitar las entradas al sistema para los usuarios.
9. El servidor no responde correctamente, por lentitud del proceso, o por intentos de accesos concorruntes mayores a los soportados.
10. Ante la ejecución de scripts o procesos mayores se congela el sistema.
11. Arroja errores con mapas de direcciones hexadecimales.

Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si existiera un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG), a menos que la dificultad apremie se debe cambiarlo inmediatamente.

Acciones a tomar:

Se debe considerer que ningún proceso debe quedar inoperativo, y se deben ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema utilizando mensajes por red y teléfono a los jefes de área.
2. El servidor debe ser apagado siguiendo el proceso establecido para apago de equipos.
3. Ubicar las memorias malogradas.

4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ello evitará que al encender el sistema, los usuarios ingresen masivamente.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

3.2.5 INCIDENTE 5 Clase de Riesgo: Equivocaciones

Grado de Negatividad: Moderado
Frecuencia de Evento: Periódico
Aleatorio Grado de Impacto: Moderado
Grado de Certidumbre: Probable

Situación actual	Acción correctiva
Las equivocaciones que se producen en forma rutinaria son de carácter involuntario.	Capacitación en el ambiente de trabajo. Instruir al nuevo usuario con el Manual del Sistema que será utilizado.
Cuando el usuario es practicante y tiene conocimientos de informática, tiene el impulso de navegar por los sistemas.	En lo posible se debe cortar estos accesos, limitando su accionar en función a su labor de rutina.
La falta de institucionalizar procedimientos produce vacíos y errores en la toma de criterios para registrar información.	Reuniones y Actas de Trabajo para el levantamiento y fortalecimiento de los procedimientos.
Notificaciones de ingresos, salidas, encargos, subrogaciones a destiempo	Se habilitaron las notificaciones masivas de cambios subrogaciones, encargos, permisos, vacaciones generadas a través del Sistema de Control de Talento Humano (RUNA) para procesamiento en la CGDIG en cuanto se generen los cambios por parte del responsable de Talento Humano.

Situación actual	Acción correctiva
Ante nuevas configuraciones se comunica a los usuarios sobre el manejo, claves, accesos y restricciones, tanto a nivel de Sistemas, Telefonía, Internet.	Enviar oficios circulares Múltiples comunicando los nuevos cambios y políticas.

Tabla: Riesgos equivocaciones

Acciones a tomar:

- Cuánto saben los empleados de computadoras o redes.
- Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
- Difusión de Manuales de Usuario y operación del correcto uso del software y el hardware a todo el personal que labora de manera directa con los equipos informáticos.

3.2.6 INCIDENTE 6 Clase de Riesgo: Fenómenos Naturales

Clase de Riesgo: Fenómenos Naturales

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Aleatorio Grado de Impacto: Grave
Grado de Certidumbre: Probable
Situación actual Acción correctiva

No se han registrado contingencias debido a fenómenos naturales suscitados en las ciudades en las que operan las oficinas de la SOT, tales como como: terremotos, inundaciones, aluviones, etc.

Medidas de prevención.

Potencialmente existe la probabilidad de sufrir inundaciones debido a lluvias que ocurren en épocas de verano que afectan a las ciudades ubicadas en la Región Costera del país.

Tenemos épocas fuertes lluvias (Fenómeno del Niño) que causas estragos en viviendas de material rústico. Las instalaciones de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo, están adecuadamente protegidas, sin embargo se debe verificar el tema del suministro eléctrico en las oficinas zonales de la SOT que operen en la región costera del país.

Al ocurrir un corte de energía el personal de vigilancia debe comunicar al personal de la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG), para desconectar el sistema de red de manera preventiva.

El ambiente donde se encuentra los Servidores principales, debe ser protegido ante las filtraciones.

Ubicación apropiada. Pero ante resultado de posibles filtraciones realizar

trabajos de mantenimiento preventivo.

Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como respaldo de aquellos que se encuentren aún en las instalaciones de la institución.

3.2.7 INCIDENTE 7 Clase de Riesgo: Accesos No Autorizados

Clase de Riesgo: Accesos NO Autorizados

Grado de Negatividad: Grave
Frecuencia de Evento: Aleatorio
Grado de Impacto: Grave
Grado de Certidumbre: Probable
Situación actual Acción correctiva

Aspectos a tomar en cuenta:

Medida	Cumplimiento
Se controla el acceso al Sistema de Red mediante la definición de "Cuenta" o "Login" con su respectiva clave	Se cumple
A cada usuario de Red se le asigna los "Atributos de confianza" para el manejo de archivos y acceso a los sistemas.	Se cumple
Cuando el personal cesa en sus funciones o es asignado a otra área, se le redefinen los accesos y autorizaciones, quedando sin efecto la primera.	Se cumple
Se forman grupos de usuarios, a los cuales se le asignan accesos por conjunto, mejorando la administración de los recursos.	Se cumple
Se acostumbra a confiar la clave de acceso (uso personal) a compañeros de área, sin medir la implicación en el caso de acceso no autorizado. En algunos casos los usuarios escriben su contraseña (Red o de Sistemas) en sitios visibles	Capacitar al personal sobre la confidencialidad de sus contraseñas, recalcando la responsabilidad e importancia que ello implica.
No se tiene un registro electrónico de Altas/Bajas de Usuarios, con las respectivas claves.	Se debe implementar

Tabla: Accesos no autorizados

Todos los usuarios sin excepción tienen un "login" o un nombre de cuenta de usuario y una clave de acceso a la red con un mínimo de cinco (5) dígitos. No se permiten claves

en blanco. Además están registrados en un grupo de trabajo a través del cual se otorga los permisos debidamente asignados por el responsable de área.

Cada usuario es responsable de salir de su acceso cuando finalice su trabajo o utilizar un bloqueador de pantalla. Ello se aplica tanto a su autenticación como usuario de Red como usuario de Sistemas de la Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo, si lo tuviere.

Acciones a tomar

- Contraseñas: Las contraseñas son a menudo, fáciles de adivinar u obtener mediante ensayos repetidos, razón por la cual en la institución se ha considerado la implementación de un número máximo de tres (3) intentos para el acceso, lo cual quiere decir que al tercer interno el equipo se bloqueará evitando el acceso.
- El Sistema de control de claves incluye la verificación de complejidad en sus contraseñas de tal forma que sean más de 8 caracteres que incluyan números, letras y caracteres especiales.
- Privilegio: En los sistemas informáticos del Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo, a cada usuario se le presenta la información que le corresponde. Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. En este punto el administrador de la red ha clasificado a los usuarios de la red en "Grupos" con el objeto de adjudicarles el nivel de seguridad y perfil adecuado.

3.2.8 INCIDENTE 8 Clase de Riesgo: Robo de Datos

Grado de Negatividad:	Grave
Frecuencia de Evento:	Aleatorio Aleatorio
Grado de Impacto:	Grave
Grado de Certidumbre:	Probable
Situación actual	Acción correctiva

Aspectos a tomar en cuenta:

El Robo de datos se puede llevarse a cabo bajo tres modalidades:

- La primera modalidad consiste en sacar "copia no autorizada" a nuestros archivos electrónicos aun medio magnético y retirarla fuera de la institución.
- La segunda modalidad y tal vez la más sensible, es la sustracción de reportes impresos y/o informes confidenciales.
- La tercera modalidad es mediante acceso telefónico no autorizado, se remite vía Internet a direcciones de Correo que no corresponden a la Gestión Empresarial.

Acciones a considerar:

Se previene a través de las siguientes acciones:

1. Accesos no Autorizado: Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

   a. Área de sensibles.
   b. Computadoras personales o terminales de la red.
   c. Información confidencial.

2. Control de acceso al Área de Sistemas: El acceso al área de Tecnología está restringido:

   a. Sólo ingresan al área el personal que trabaja en el área.
   b. El ingreso de personas extrañas solo podrá ser bajo una autorización.

3. Acceso Limitado a los Terminales de Administración: Cualquier terminal que puede ser utilizada como acceso a los datos de un Sistema, debe considerar las siguientes restricciones:

   a. Determinación de los períodos de tiempo para los usuarios o las terminales.
   b. Designación del usuario por terminal.
   c. Limitación del uso de programas para usuario o terminales.
   d. Límite de tentativas para la verificación del usuario, tiempo de validez de las señas, uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 minutos)

4. Niveles de Acceso: Los programas de control de acceso deben identificar a los usuarios autorizados para el uso de determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

   a. Nivel de consulta de la información - privilegio de lectura.
   b. Nivel de mantenimiento de la información - el concepto de mantenimiento de la información consiste en: Ingreso, Actualización, Borrado.

3.2.9 INCIDENTE 9 Clase de Riesgo: Manipulación y Sabotaje

Grado de Negatividad:	Grave
Frecuencia de Evento:	Aleatorio
Grado de Impacto:	Grave
Grado de Certidumbre:	Probable
Situación actual	Acción correctiva

Existe el problema de la inestabilidad laboral, la misma que podría obligar a personas frustradas, o desilusionadas a causar daños físicos y lógicos en el sistema de información de la institución. Esto se puede traducir desde el registro de operaciones incorrectas por parte de los usuarios finales, hasta la operación de borrar registros en el sistema y conductas de sabotaje.

La protección contra el sabotaje requiere:

- Una selección rigurosa del personal.

- Buena administración de los recursos humanos
- Buenos controles administrativos
- Buena seguridad física en los ambientes donde están los principales componentes del equipo.
- Asignar a una persona la responsabilidad de la protección de los equipos en cada área.

Es conveniente la comunicación anticipada del personal que será reubicado y/o cesado con el objeto de retirar los derechos de operación de escritura para otorgarle los derechos de consulta antes de desactivar la cuenta.

Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado.

El peligro más temido por los centros de Procesamiento de Datos, es el sabotaje.

Las Instituciones que han intentado implementar Programas de Seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un trabajador o un sujeto ajeno a la propia institución. Un acceso no autorizado puede originar sabotajes.

Los riesgos y peligros deben ser identificados y evaluados, para conocer las posibles pérdidas y para que pueda ponerse en práctica los adecuados métodos de prevención.

Una mejora en la seguridad produce, a menudo, importantes beneficios secundarios. Por ejemplo, el cambio de metodología aplicada a determinadas operaciones conduce frecuentemente a una reducción del índice de errores, a una mejora en calidad, a una mejor planificación y a resultados más rápidos.

No existen un plan idóneo o una recomendación simple para resolver el problema de la seguridad. Realmente no es una situación estática un problema "puntual", sino que requiere un constante y continuo esfuerzo y dedicación.

Acciones a tomar:

A continuación se detallan algunas medidas a considerar para evitar acciones hostiles:

a. Mantener ética profesional en el trabajo, y personal con los compañeros y autoridades.
b. Mantener respaldos de archivos digitales en BackUp, en dispositivos externos custodiados.
c. Planear para probar los respaldos (BackUp) de los servicios de procesamiento de datos.
d. Identificar y establecer operaciones críticas prioritarias cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
e. Usar rastros de auditorías o registros cronológicos (logs) de transacción como medida de seguridad.

Cuando la información eliminada se pueda volver a capturar, se procede con lo

siguiente:

a. Capturar los datos faltantes en las bases de datos de los sistemas.
b. Revisar y probar la integridad de los datos.

La eliminación de la información, puede volverse a capturar en la mayoría de los casos, sin embargo en algunas ocasiones, las pérdidas demandan demasiado tiempo requerido para el inicio de las operaciones normales, por tal motivo es recomendable acudir a los respaldos de información y restaurar los datos pertinentes, de esta forma las operaciones del día no se verán afectados.

3.2.10 INCIDENTE 10 Clase de Riesgo: Acción de Virus Informático

Grado de Negatividad:	Muy Severo
Frecuencia de Evento:	Continuo
Grado de Impacto:	Grave
Grado de Certidumbre:	Probable
Situación actual	Acción correctiva

De manera actual no se cuenta con un software antivirus Institucional, ya que se depende de la certificación prosupuestaria y aval del Ministerio de Finanzas para el inicio de proceso de adquisición.

En cuanto se cuente con el software de antivirus, se instalará de manera inmediata en las estaciones de trabajo y servidores de la SOT.

Considerando que en la Institución aún no se dispone del licenciamiento antivirus para los equipos informáticos y servidores de la SOT, se ha optado por productos que ofrece el mercado de software libre y licencias temporales, con el objeto de mitigar el acceso de virus que puedan ocasionar daños a la red institucional.

Acciones a tomar:

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidores de Data Center:

- El acceso a la navegación en los servidores es restringida para evitar la descarga de archivos, programas y paquetes que puedan contener virus o troyanos que afectarían la operación de los servidores que alojan los multiples sistemas y servicios tecnológicos institucionales.
- Se mantiene desplegada una versión free de antivirus para el aseguramimento de los servidores, con el objeto de evitar el acceso de archivos infectados.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es considerar que la infección fue realizada desde alguna de las estaciones a través de las cuales se accede al servidor, mismas que serán revisadas para la depuración y limpieza del equipo de los virus.

Para computadoras fuera de red:

- Utilizar los discos de instalación que contengan sistema operativo igual o mayor en versión al instalado en el computador infectado.
- Insertar el disco de instalación antivirus, luego instalar el sistema operativo, de tal forma que revise todos los archivos y no sólo los ejecutables.
- En el caso de que se identifiquen virus, se debe proceder con el bloqueo del virus enviándolo a cuarentena manual en el caso de que el propio sistema antivirus no lo realice.
- Recomendar realizar el borrado de los archivos infectados.
- Considerar los archivos infectados que no se borran para una nueva depuración y escaneo de virus.
- Iniciar nuevamente la opción de escaneo e identificación de virus en el equipo infectado.
- Finalizado el escaneado, reconstruir el Master Boot del disco duro.

4. ANÁLISIS DE LAS FALLAS EN LA SEGURIDAD

Las fallas en la seguridad de la información y por consiguiente de los equipos informáticos, puede ocasionar la divulgación de información sensible de la institución o de sus colaboradores, razón por la cual es importante considerar la seguridad de la información en los siguientes aspectos:

- Negar el acceso a los datos a aquellas personas que no tengan derecho a ellos.
- Garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

Protecciones actuales:

Se ejecutan las siguientes acciones:

- Se realizan copias de los archivos que son vitales para la institución.
- Al robo común se cierran las puertas de entrada y ventanas.
- Al vandalismo, se cierra la puerta de entrada.
- A la falla de los equipos, se mantienen garantías vigentes de los equipos tecnológicos.
- Al daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus.
- A las equivocaciones, los empleados tienen buena formación. Cuando se requiere personal temporal se intenta conseguir a empleados debidamente preparados, o en el caso de suscitarse un error el mismo es comunicado a las áreas correspondientes para conocimiento y gestión.
- A terremotos, no es posible proteger la instalación frente a estos fenómenos. El presente Plan de contingencias da pautas al respecto.
- Al acceso no autorizado, se cierra la puerta de entrada. Varias computadoras disponen de llave de bloqueo del teclado.
- Al robo de datos, se cierra la puerta principal y gavetas de escritorios. Varias computadoras disponen de llave de bloqueo del teclado.
- Al fuego, en la actualidad se encuentran instalados extintores, en sitios

estratégicos y se brindara entrenamiento en el manejo de los extintores al personal, en forma periódica.

- Se incentiva al personal a una cultura organizacional cero papeles y escritorios limpios, lo cual quiere decir que no deben imprimir documentos de manera innecesaria ya que los mismos pueden ser direccionados a través del Sistema de Gestión Documenal Interno (SIGDO), o servicio de correo electrónico institucional, y los documentos impresos sensibles no deben ser abandonados sobre los escritorios o en los puestos de trabajo sin la debida seguridad que precautele la confidencialidad e integridad.

5. SEGURIDAD DE LA INFORMACIÓN

La Seguridad de información y por consiguiente de los equipos informáticos, si no es aplicada concientemente en la institucióin puede llegar a afectar la imagen institucional, incluyendo la vida privada de las personas.

Ladrones, manipuladores, saboteadores, espías, entre otros, reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y a menudo es vulnerable a cualquier ataque.

La Seguridad de información tiene tres directivas básicas que actúan sobre la Protección de Datos, las cuales ejercen control de:

- Lectura: Consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales y mantenimiento de la seguridad en el caso de datos institucionales.

- Escritura: Garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad que se les ha confiado.

- Empleo de esa información

  El Secreto se logra cuando no existe acceso a todos los datos sin autorización. La privacidad se logra cuando los datos que puedan obtenerse no permiten el enlace a individuos específicos o no se pueden utilizar para imputar hechos acerca de ellos.

En la SOT se han definido los dispositivos de seguridad requeridos, los cuales constan en los diseños de la arquitectura tecnológica de la institución para la mitigación de riesgos y amenazas que puedan atentar contra la seguridad de la información:

1. Prevención de acceso no autorizado: Los equipos tecnológicos, sistemas de información y controles de acceso institucionales, cuentan con las medidas de seguridad para verificación de inicios de sesión y control de accesos, para evitar la filtración de terceros no autorizados.

2. Control de acceso a la CGDIG: La libertad de acceso al área de operación central de la Institución que se encuentra custodiada por la Coordinación General de

Desarrollo de Softwarea e Infraestructura de Datos Geoespaciales (CGDIG), puede crear un significativo problema de seguridad. El acceso al área del Data Center Institucinal únicamente es otorgado al personal de la Dirección de Infraestructura y Mantenimiento de Datos Geoespaciales de la CGDIG, quienes realizan el registro de huellas para el ingreso al Data Center. Cuando un tercero a la unidad o institución desea ingresar al Data Center, se registra la solicitud en una bitácora de accesos para terceros, quienes siempre irán acompañados por el responsable designado de la CGDIG.

a) Para personas visitantes, el persona de vigilancia de la SOT debe entregar una credencial de visitante con la identificación clara del piso al que ingresará.
b) El personal de la SOT debe portar la credencial institucional siempre dentro de la institución, y en el caso que requiera accede al área sensible del Data Center, primero solicitará el respectivo permiso con el justificativo necesario a la Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales, quién confirmará o negará el acceso.

3. Acceso limitado computadoras personales o terminales de la red: Las terminales que son dejadas sin protección pueden ser mal usadas. Cualquier Terminal puede ser utilizada para tener acceso a los datos de un sistema controlado. Todos los equipos portátiles y de escritorio de la SOT deben ser bloqueados cuando el funcionario responsable de dichos equipos se encuentre lejos de su puesto de trabajo.

4. Control de acceso a la información confidencial: Sin el debido control, cualquier usuario puede encontrar la forma de lograr acceso al Sistema de Red, a una base de datos o descubrir información clasificada. Para el control de acceso en la red la Institución cuenta con el Firewall de Chekpoint.

5. Programas de control a los usuarios de red: El sistema Operativo residente en los servidores de la CGDIG es Windows Server 2016. A través del Servicio de "Active Directory" permite administrar a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

6. Palabra de acceso (password): El password es indispensable para el ingreso a cualquier servidor, equipo, Sistema o base de datos. El password constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados. La identificación del usuario debe ser muy difícil de imitar y copiar.

   Los Sistema de Información deben ser cerrados después de tres (3) intentos no válidos de acceso. Las claves de acceso deben incluir una letra mayúscula, letras minúsculas y algún número o caractér especial, y deben ser recordadas por el funcionario pero no anotadas en algún documento o cuaderno al que pueda accede cualquier otra persona. La clave de acceso al Sistema es utilizada para entrar a la red, sistemas de información, bases de datos, aplicaciones, entre otros.

   La forma común de intentar descubrir una clave es de dos maneras:

   - Observando el ingreso de la clave

- Utilizando un método de ensayo y error para introducir posibles claves de acceso y lograr entrar.

En todo proceso institucionnal es recomendable que el colaborador cambie de forma periódica el "password" de acceso a su cuenta (red, correo y sistemas informáticos).

7. Niveles de Acceso: Las políticas de acceso aplicadas, deben identificar los usuarios autorizados a emplear determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes formas.

   Cada palabra clave debe tener asignado uno de los niveles de acceso a la información o recursos de red disponibles en el institución. La forma fundamental de autoridad la tiene el Administrador de Redes con derechos totales. Entre otras funciones puede autorizar nuevos usuarios, otorgar derechos para modificar estructuras de las Bases de Datos, entre otros.

   De acuerdo a ello se tienen los siguientes niveles de acceso a la información:

   Nivel Concepto: Consulta de la información. El privilegio de lectura está disponible para cualquier usuario y solo se requiere presentaciones visuales o reportes. La autorización de lectura permite leer pero no modificar la Base de Datos.

   El mantenimiento de información, permite el acceso para agregar nuevos datos, pero no modifica los ya existentes, los datos no son modificables y tampoco pueden ser eliminados.

   No está permitida la eliminación de datos, ya que estos son registros históricos, así como las cuentas de usuarios y registros de actividades, no pueden ser editados, modificados ni borrados. Los usuarios unicamente se inactivan.

DESTRUCCIÓN:

Sin las adecuadas medidas de seguridad la institución puede estar a merced no solo de la destrucción de la información sino también de la destrucción de sus equipos informáticos. La destrucción de los equipos puede darse por una serie de desastres como son: incendios, inundaciones, sismos, posibles fallas eléctricas, sabotaje, entre otros.

Cuando se pierden los datos y no hay copias de seguridad, se tendrá que recrear archivos, bases de datos, documentos o trabajar sin ellos.

Está comprobado que una gran parte del espacio en disco está ocupado por archivos de naturaleza histórica, que es útil tener a mano pero no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia conservados como documentos de referencia o plantilla. Si se guarda una copia de seguridad de estos archivos las consecuencias de organización pueden ser mínimas.

Los archivos electrónicos contables son de disposición diferente, ya que volver

a crearlos puede necesitar de mucho tiempo y costo. Generalmente la institución recurre a esta información para la toma de decisiones financieras. Es importante considerer que los registros contables son respaldados de manera física y digital por el área responsable que es la Coordinación General Administrativa Financiera (CGAF).

REVELACIÓN O DESLEALTAD:

La información sensible de la institución puede ser conocida por personas ajenas a la institución por filtrado de información, y puede ser accedida por las siguientes causas:

- Abandono u olvido de documentos físicos en sitios de trabajo o equipos de impresión, sin los resguardos o seguridad que precautele la confidencialidad de los mismos.
- Abandono u olvido de cds, medios de almacenamiento externos, entre otros, que pueden ser tomados por terceros para revision de información sensible almacenada en dichos dispositivos.
- Difusión de información institucional no oficial que pudo ser tergiversada y manipulada por terceros.

El material de papel en la plataforma de descarga de la basura puede ser la fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Para tener una mayor seguridad de protección de la información residual y segregada, esta deberá ser destruida, eliminada físicamente, manualmente o mecánicamente (picadoras de papel).

Desafortunadamente, es muy común ver en las áreas de trabajo grandes volúmenes de información sin resguardo, razón por la cual en la SOT se está implementado una cultura institucional "cero papeles" y de seguridad de la información con el objeto de concientizar a los colaboradores en la importancia del cuidado de los datos e información.

MODIFICACIONES:

En la institución no está permitida la modificación, manipulación o borrado de información, datos o registros, gestionados, procesados o almacenados en los sistemas de información de la SOT, por lo cual se han establecido algunos procedimientos para el control de los datos e información digital:

- Los programas de aplicación: Cuentan con controles que evitan las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionales a los datos o a su uso no autorizado.
- La información en Bases de Datos: Como medidas de Seguridad, para proteger los datos en el sistema, el responsable de la base de datos genera reportes del estado de la base de datos para el control histórico y verificación de los registros.
- Generación de backups de bases de datos: Contra la perdida o modificación de datos se efectúan copias de seguridad de la base de datos y registros de los sistemas de información que son almacenados en un equipo externo para la contingencia, mismo que será instalado en la

oficina zonal de Quito de la SOT.

- Los usuarios: los usuarios deben ser concientizados de la variedad de formas en que los datos pueden perderse o deteriorarse. Se está desarrollando una campaña educative a través de la cual se pueda profundizar con una serie de seminarios y reforzarse con carteles y circulares relacionados al tema "Seguridad de la Información".

Para la realización de las Copias de Seguridad se tiene que tomar algunas decisiones previas como:

- ¿Qué soporte de copias de seguridad se va utilizar?
- ¿Se van a usar dispositivos especializados para copia de seguridad?
- ¿Con que frecuencia se deben realizar las copias de seguridad?
- ¿Cuáles son los archivos a los que se le sacará la copia de seguridad y donde se almacenará?

La Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales (CGDIG), establecerá Directivas y Reglamentos en estas materias, para que los usuarios tomen conocimiento y conciencia de sus responsabilidades.

La institución debe tener en cuenta los siguientes puntos para la protección de los datos de una posible contingencia:

- Realizar copias de seguridad de la información, acogiendo políticas internacionales de Seguridad de la Información tal como la expuesta en la Norma Internacional ISO/IEC 27001:2013.
- Establecer el equipamiento indispensable para la generación de copias de seguridad de la información, tales como (equipos adecuados, disponibilidad, suministros, horarios, responsables, entre otros).
- Establecer como Política que las copias de seguridad son obligatorias.

Fin del documento

Atentamente,

SUPERINTENDENCIA DE ORDENAMIENTO TERRITORIAL, USO Y GESTIÓN DEL SUELO

Coordinación General de Desarrollo de Software e Infraestructura de Datos Geoespaciales

Mgs. Mónica Uyana García
COORDINADORA GENERAL DE DESARROLLO DE SOFTWARE E INFRAESTRUCTURA DE DATOS GEOESPACIALES - CGDIG
Superintendencia de Ordenamiento Territorial, Uso y Gestión del Suelo