| | |
|---|---|
| **PROCESO:** SISTEMAS | **SUBPROCESO (PROCEDIMIENTO):** PLAN DE CONTINGENCIA, CONTINUIDAD Y SEGURIDAD DE LOS SISTEMAS DE LA CAJA. |
| **RESPONSABLE:** JEFE DE SISTEMAS | |

## 1. INFORMACIÓN GENERAL DEL PROCEDIMIENTO

**OBJETIVO:** Propender por la seguridad, protección y conservación de los activos de la empresa, minimizando los posibles riesgos que llegasen a presentarse.

**ALCANCE:** Este procedimiento aplicara para todos los procesos que componen COMFACASANARE.

**DEFINICIONES:**

**ATAQUES INFORMATICO:** Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red.

**DESASTRES NATURALES:** hace referencia a las enormes pérdidas materiales ocasionadas por eventos o fenómenos naturales.
**FIREWALL:** programa encargado de analizar tanto el tráfico entrante como saliente de un equipo, con el fin de bloquear determinados puertos y protocolos que potencialmente podrían ser utilizados por las aplicaciones.

**PIRATAS INFORMATICOS:** Aquellos hackers que emplean sus conocimientos con fines ilegales o inmorales.

**PLAN DE EMERGENCIA:** Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

**PLAN DE RECUPERACION:** Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

**PLAN DE RESPALDO:** Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad atenuar los efectos adversos de la amenaza.

**RIESGOS:** amenaza concreta que puede materializarse en cualquier momento.

**SEGURIDAD:** protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida).

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

**SPAM:** mensajes de correo electrónico comercial no solicitado.

**VIRUS:** En informática, pequeño software que, al igual que un virus biológico, infecta a una computadora y se propaga en ella con diversos propósitos como daño, robo de información, molestia, etc. y por lo general intenta pasar desapercibido por el usuario el mayor tiempo posible.

**DOCUMENTOS DE REFERENCIA:** Ley 21 de 1982, Ley 789 de 2002, Código de comercio, Código Civil, Decreto 341 de 1988, Decreto 2463 de 1983, Reglamento Interno de Trabajo, Plan de Medios, Manuales de funciones, Procesos y Procedimientos

**CONDICIONES GENERALES:**
N.A

## 2. INFORMACIÓN ESPECÍFICA DEL PROCEDIMIENTO

| No. | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | | REGISTROS | PUNTOS DE CONTROL |
|---|---|---|---|---|---|---|
| | | | DEPENDENCIA O UNIDAD DE GESTIÓN | CARGO Y/O PUESTO DE TRABAJO | | |
| 1 | Análisis | En esta fase se identifican los posibles eventos adversos a los cuales está expuesta la empresa, con la ayuda de los descritos en el PETIC se analiza las vulnerabilidades y se describen las posibles soluciones previstas ante los inconvenientes que llegasen a ocurrir. | Subdirección Operativa | Jefe de sistemas | N.A | |

## 2. INFORMACIÓN ESPECÍFICA DEL PROCEDIMIENTO

| No. | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | | REGISTROS | PUNTOS DE CONTROL |
|---|---|---|---|---|---|---|
| | | | DEPENDENCIA O UNIDAD DE GESTIÓN | GARGO Y/O PUESTO DE TRABAJO | | |
| 2 | Planeación | Identificados los riesgos potenciales se definen las acciones a realizar y se ponen en marcha algunos planes:<br><br>**PLAN DE EMERGENCIA:** Contempla las acciones preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización. Con la ayuda de las Brigadas pertenecientes al COPASO se estudian medidas por adoptar.<br><br>**PLAN DE RESPALDO:** Consiste en atenuar los efectos adversos de la amenaza, para evitar perdida de información.<br><br>**PLAN DE RECUPERACION:** Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la ocurrencia. | Subdirección Operativa | Jefe de sistemas Brigadas. | Registro de Novedades diarias FSIS002 | |
| 3 | Restauración | Esta etapa se deja el sistema como estaba funcionando inicialmente. Se están evaluando si las soluciones actuales son las adecuadas para la restauración del sistema en caso de presentarse alguna eventualidad. | Subdirección operativa | Jefe de sistemas. | | Sistema restaurado |

## 2. INFORMACIÓN ESPECÍFICA DEL PROCEDIMIENTO

| No. | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | | REGISTROS | PUNTOS DE CONTROL |
|---|---|---|---|---|---|---|
| | | | DEPENDENCIA O UNIDAD DE GESTIÓN | GARGO Y/O PUESTO DE TRABAJO | | |
| 4 | Implementación del firewall | Configuración básica del firewall | Subdirección operativa | Jefe de Sistemas | N.A | |
| 5 | Crear política de seguridad | Personal encargado en virtud de la política de seguridad establecida, se asignan roles de acceso a la información, se proveen permisos y soportes informáticos, para controlar la entrada y salida de información, identificación y resolución de incidencias | Subdirección operativa | Jefe de Sistemas | Registro del sistema | |
| 6 | Crear directiva de uso aceptable | Una directiva de uso aceptable es un documento en el que se informa a los empleados de lo que pueden y no pueden hacer en los equipos de la empresa. Ponga por escrito las normas que espera que se cumplan. Puede describir su política sobre la creación de contraseñas, indicar la frecuencia de cambio de contraseñas o mencionar el riesgo que supone abrir archivos adjuntos de correo electrónico de remitentes desconocidos. También puede incluir la prohibición de Instalar software no autorizado en los equipos. En este documento, que debe ser firmado por todos los empleados, tienen que constar las sanciones (en casos extremos, incluso el despido) por contravenir esas normas. En su calidad de propietario o director del negocio, también deberá firmar una copia de la directiva. Si la directiva es | Subdirección operativa | Jefe de Sistemas, técnico y/o auxiliar. | Comunicación interna | |

**2. INFORMACIÓN ESPECÍFICA DEL PROCEDIMIENTO**

| No. | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | | REGISTROS | PUNTOS DE CONTROL |
|---|---|---|---|---|---|---|
| | | | DEPENDENCIA O UNIDAD DE GESTIÓN | GARGO Y/O PUESTO DE TRABAJO | | |
| | | larga y detallada, ayude a los empleados a recordar los puntos principales con un resumen de una página que puede distribuir y colocar cerca de sus estaciones de trabajo. | | | | |
| 7 | Concientizar a los empleados | Distribuir proactivamente a través de comunicaciones periódicas las actualizaciones en las políticas de seguridad | Subdirección operativa | Jefe de Sistemas. | Capacitación | |
| 8 | Proteger de los virus y el software espía | Se debe disponer de protección antivirus en todos sus equipos de escritorio y portátiles. El software antivirus examina el contenido de los archivos en su pc en busca de indicios de virus. Cada mes aparecen cientos de virus nuevos, por lo que hay que actualizar periódicamente los antivirus con las últimas definiciones para que el software pueda detectar los nuevos virus. | Subdirección operativa | Jefe de Sistemas, técnico y/o auxiliar | N.A | Listado de equipos con antivirus |
| 9 | Evitar correos no deseados (spam) | Si recibe un correo electrónico de un remitente desconocido se debe eliminar sin abrirlo, puede contener virus. Tampoco responda al mismo, ya que estaría confirmando que su dirección es correcta y está activa. No se debe realizar envío de publicidad a aquellas personas que no hayan autorizado previamente el consentimiento de recibir publicidad. Adoptar medidas de protección frente al correo electrónico no deseado. | Subdirección operativa | Jefe de Sistemas, técnico y/o auxiliar | Comunicación interna | |

## 2. INFORMACIÓN ESPECÍFICA DEL PROCEDIMIENTO

| No. | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | | REGISTROS | PUNTOS DE CONTROL |
|---|---|---|---|---|---|---|
| | | | DEPENDENCIA O UNIDAD DE GESTIÓN | GARGO Y/O PUESTO DE TRABAJO | | |
| | Licenciar todos los programas | El uso de software ilegal además de generar riesgos de carácter penal, también puede generar problemas en la seguridad de la información, lo que lo que conlleva a pérdidas en la rentabilidad y productividad de la organización. El software legal ofrece garantía y soporte del fabricante. | Subdirección operativa | Jefe de Sistemas, técnico y/o auxiliar | Hoja de vida equipos FSIS003 (GLPI) | |
| 11 | Navegación Segura | Acceder únicamente a sitios de confianza. Analizar con un antivirus todo lo que descarga antes de ejecutarlo en su equipo. No explorar nunca sitios Web desde un servidor. Mantener actualizado su navegador a la última versión. Configurar el nivel de seguridad de su navegador según sus preferencias. Descargar los programas desde los sitios oficiales para evitar suplantaciones maliciosas | Subdirección operativa | Jefe de Sistemas, técnico y/o auxiliar | N.A. | |
| 12 | Utilizar contraseñas seguras. | Informar a los empleados de la importancia de las contraseñas es el primer paso para convertir las contraseñas en una valiosa herramienta de seguridad de la red, ya que dificultan la suplantación de su usuario. Es decir, no se debe dejar en cualquier parte ni se debe compartir. Características de una contraseña "segura": Una longitud de ocho caracteres como mínimo; cuanto más larga, mejor. Una combinación de letras mayúsculas y minúsculas, números y símbolos. Se debe | Subdirección operativa | Jefe de Sistemas | Comunicación interna | Listado de contraseñas en sobre cerrado |

## 2. INFORMACIÓN ESPECÍFICA DEL PROCEDIMIENTO

| No. | ACTIVIDAD | DESCRIPCIÓN | RESPONSABLE | | REGISTROS | PUNTOS DE CONTROL |
|---|---|---|---|---|---|---|
| | | | DEPENDENCIA O UNIDAD DE GESTIÓN | GARGO Y/O PUESTO DE TRABAJO | | |
| | | cambiar cada 90 días como mínimo y, al cambiarla, debe ser muy distinta de las contraseñas anteriores. No utilice datos personales | | | | |
| 13 | Realizar copias de seguridad | La realización de copias de seguridad de los datos significa crear una copia de ellos en otro medio. Por ejemplo, puede grabar todos los archivos importantes en un CD-ROM o en otro disco duro. Es recomendable probar las copias de seguridad con frecuencia mediante la restauración real de los datos en una ubicación de prueba. | Subdirección operativa | Jefe de Sistemas | N.A | |

| INDICADORES | OPORTUNIDADES Y AFECTACIONES DE LAS PARTES INTERESADAS | FORMATO DE DOCUMENTOS |
|---|---|---|
| N.A | Ver mapa de Riesgos y Matriz de relación procesos, partes interesadas, política y objetivos de calidad | **FSIS002** REGISTRO DE NOVEDADES DIARIAS |

| Elaboró | Revisó | Aprobó |
|---|---|---|
| Nombre:<br>JORGE ENRIQUE OLMOS DEL VALLE<br><br>Cargo:<br>Jefe de Sistemas | Nombre:<br>DIANA CAROLINA FONSECA GARAVITO<br><br>Cargo:<br>Subdirectora Operativa | Nombre:<br>GUSTAVO E. AYALA LEAL<br><br>Cargo:<br>Director |

## ANEXO 01. FLUJOGRAMA DEL PROCEDIMIENTO