**FC - TECH**



**Manual de seguridad**

Contenido

[INTRODUCCION 3](#_Toc23855025)

[Objetivo 3](#_Toc23855026)

[DEFINICIONES TEÓRICAS 3](#_Toc23855027)

[Plan de seguridad 3](#_Toc23855028)

[Políticas de seguridad 3](#_Toc23855029)

[Seguridad Informática 3](#_Toc23855030)

[Sistema de información 3](#_Toc23855031)

[Para afrontar el establecimiento de un sistema de seguridad es necesario conocer: 4](#_Toc23855032)

[Tipos de Seguridad 4](#_Toc23855033)

[Propiedades de un sistema de información seguro 4](#_Toc23855034)

[Definiciones conceptuales 4](#_Toc23855035)

[Alcance del Plan de Seguridad Informática 4](#_Toc23855036)

[RELEVAMIENTO 5](#_Toc23855037)

[Análisis - FODA 5](#_Toc23855038)

[Análisis de riesgo 6](#_Toc23855039)

[POLÍTICAS DE SEGURIDAD INFORMÁTICA 7](#_Toc23855040)

[Responsables 7](#_Toc23855041)

[Medidas y procedimientos de protección Física 8](#_Toc23855042)

[Medidas y procedimientos de protección lógicas 9](#_Toc23855043)

[**REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** 12](#_Toc23855044)

[Plan de Contingencia 14](#_Toc23855045)

[**1. INCENDIO** 14](#_Toc23855046)

[**2. FALLAS EN LOS EQUIPOS, DAÑOS DE ARCHIVOS.** 14](#_Toc23855047)

[**3. EQUIVOCACIONES, DAÑOS DE RCHIVOS.** 14](#_Toc23855048)

[**4. ACCESO NO AUTORIZADO, FILTRACIÓN DE** 14](#_Toc23855049)

[**INFORMACIÓN.** 14](#_Toc23855050)

[**5. VIRUS Y DAÑO DE ARCHIVOS** 15](#_Toc23855051)

[Evaluación de daños 15](#_Toc23855052)

[Contención y mitigación 15](#_Toc23855053)

[Evaluación y resultados 15](#_Toc23855054)

[Recomendaciones: 16](#_Toc23855055)

# INTRODUCCION

Hoy en día vivimos en un mundo de constantes cambios, donde la era digital ha obligado a instituciones y empresas, a implementar sistemas informáticos que contribuyan en mejorar los procesos o actividades en la que estas operan, convirtiéndose así en la parte fundamental del desarrollo de la organización, pero vale hacer hincapié y recordar que no solo se trata de poseer activos informáticos y ya se solucionó el problema, sino que también se deben de establecer normas que regulen el uso de las mismas, y minimicen el riesgo de seguridad tanto por ataques internos y externos a la que está expuesta toda organización.

Es así que un Plan de Seguridad Informática constituye un documento fundamental para establecer políticas de seguridad informática y debe ser de obligatorio cumplimiento para todo el personal que trabaja en una empresa.

Siguiendo estos principios, en el presente trabajo se realizó un diagnóstico situacional, que constituyó en una evaluación total de los bienes informáticos: software, hardware, unidades de red, y niveles de accesibilidad al área de tecnología, adquisición, soporte, implementación y supervisión de los recursos informáticos.

Identificando todos los riesgos, se elaboró el plan de seguridad, donde se estableció algunas propuestas de seguridad, buenas prácticas y recomendaciones para corregir algunos problemas que podrían ocurrir.

# Objetivo

El objetivo de este trabajo es realizar una propuesta de plan de seguridad informática para la empresa FC-TECH y así proteger los bienes tecnológicos (Hardware y software) con los que cuenta la empresa. Es necesario que las entidades aseguren la **confidencialidad**, **integridad** y **disponibilidad** de la información vital corporativa. Para lograrlo se plantearon los siguientes objetivos específicos:

• Realizar el estudio actual del estado situacional de los bienes informáticos y de la información de tecnología de la de empresa.

• Realizar el análisis de riesgo de la seguridad informática de empresa.

• Proponer políticas y medidas de seguridad informática para la empresa.

•Proponer un plan de contingencia, para proteger temporalmente los bienes informáticos de la empresa.

Las mismas que puedan garantizar la protección y/o reducción del impacto que puedan causar alguna amenaza.

# DEFINICIONES TEÓRICAS

## Plan de seguridad

Conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.

## Políticas de seguridad

Una política de seguridad consiste de enunciados que clasifican los riesgos de información, identifican los objetivos de seguridad aceptables y también los mecanismos para lograr estos objetivos.

## Seguridad Informática

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta.

## Sistema de información

Podemos plantear la definición técnica de un sistema de información como un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de control en una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores del conocimiento a analizar problemas, visualizar temas complejos y crear nuevos productos.

## Para afrontar el establecimiento de un sistema de seguridad es necesario conocer:

* Cuáles son los elementos que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables directivos de la organización para la que se hace el estudio de riesgos y mediante la apreciación directa.
* Cuáles son los peligros que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aprobados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreo sobre el mismo
* Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible.

## Tipos de Seguridad

* **Activa:** Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. Ejemplos: impedir el acceso a la información a los usuarios no autorizados mediante introducción de usuarios y contraseñas; evitar la entrada de virus instalando un antivirus; impedir mediante encriptación, la lectura no autorizada de mensajes.
* **Pasiva:** Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos.

## Propiedades de un sistema de información seguro

Se considera seguro a un sistema que cumple con las siguientes propiedades:

* **Integridad:** Evitar que personas no autorizadas puedas acceder a la información.
* **Confidencialidad:** Guardar la totalidad de la información, cuyo contenido debe permanecer inalterado a menos que sea modificado por personal autorizado.
* **Disponibilidad**: La información y los recursos relacionados deben estar disponible para el personal autorizado.

## Definiciones conceptuales

**Amenaza**: Se entiende por amenaza a la presencia de uno más factores de diversos índoles (Personas, maquinas o sucesos) que de tener oportunidad atacan al sistema produciéndole daños Aprovechando de su nivel de vulnerabilidad.

**Hacker**: Es un individuo que intenta obtener acceso sin autorización a un sistema computacional.

**Riesgo**: Se denomina riesgo a la posibilidad que se materialice o no la amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

**Seguridad**: se refiere a las políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso sin autorización, la alteración, el robo o el daño físico a los sistemas de información.

**Virus**: Es un programa de software malintencionado que se une a otros programas de software o archivos de datos para poder ejecutarse, por lo general sin el conocimiento o permiso del usuario.

**Vulnerabilidad**: Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a la misma amenaza.

# Alcance del Plan de Seguridad Informática

El presente plan de seguridad informática tiene un alcance total del personal de todas las áreas de la empresa FC-Tech. Para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos.

# RELEVAMIENTO

Se tendrá en cuenta ítems referentes a los distintos aspectos de seguridad.

|  |  |
| --- | --- |
| **Nivel** | **PREGUNTAS** |
| **Físico** | 1. ¿Hay personal de seguridad? 2. ¿Existe registro del ingreso de personal? 3. ¿Cuentan con protección contra incendios? 4. ¿Cuentan con red LAN? 5. ¿Cuentan con red WAN? Como es la interconexión de datos? 6. ¿Dónde se encuentra alojado el servidor? ¿Quién tiene acceso al mismo? 7. ¿Cuentan con wifi? ¿Cuáles son las restricciones? 8. ¿Cuentan con área de soporte técnico? ¿Interna o tercializada? 9. ¿Poseen un área o responsable de seguridad informática? 10. ¿Existe un comité de seguridad? 11. ¿Cómo reportan incidentes? 12. ¿Cuentan con un plan de acción ante posibles amenazas? 13. ¿Existe un monitoreo y control? 14. ¿Capacitan a sus empleados para el uso correcto de los sistemas? |
| **Lógico** | 1. ¿Los empleados trabajan de forma remota? ¿Tienen acceso a datos internos? ¿De qué forma? 2. ¿Las computadoras están todas dentro de un dominio? 3. ¿Cómo ingresan los usuarios a las computadoras? 4. ¿La información que manejan los usuarios se almacenan de forma local en las pc o en servidores/nube? 5. ¿Utilizan dispositivos extraíbles(USB/CD/Memorias) como medio de transmisión/almacenamiento de datos? 6. ¿Realizan backups de la información? ¿Con que regularidad? 7. ¿Las computadoras cuentan todas con antivirus? ¿Tienen licencia del mismo? 8. ¿Los programas que utilizan están licenciados? 9. ¿Los softwares propios de la empresa son públicos o internos? 10. ¿Posee documentación de las aplicaciones que utiliza? |

# Análisis - FODA

|  |  |
| --- | --- |
| **OPORTUNIDADES** | **AMENAZAS** |
| - Mejorar la variedad y calidad de cursos de capacitación para el personal especializado  -implementar políticas seguridad de la información.  - Mejorar el uso de los recursos existentes | - No hay plan de acción ante amenazas.  –Los empleados se conectan remotamente  -Ataques cibernéticos |
| **FORTALEZAS** | **DEBILIDADES** |
| - Equipamiento robusto.  -Área de seguridad que cuentan con cámaras y  registros de ingreso a la organización.  -Red Lan y Wan recientenemente instaladas.  -Buena ubicación del centro de computos | -No existe un sistema administrativo de control que verifique las actividades que realiza informática  - No se ofrece capacitación para el personal  Políticas de seguridad  Comité de seguridad |

# 

# Análisis de riesgo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Referencias:** | | | | |
| **Muy alto** | **Alto** | **Medio** | **Bajo** | **Muy Bajo** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RESUMEN DE ANALISIS DE RIESGOS** | | | | | |
| **RIESGO** | **FACTOR DE RIESGO** | | | | |
| **MUY**  **BAJO** | **BAJO** | **MEDIO** | **ALTO** | MUY ALTO |
| Incendio |  | x |  |  |  |
| Vandalismo, daño de equipos y  archivos. |  | X |  |  |  |
| Fallas en los equipos. |  |  |  | x |  |
| Capacitación al personal |  |  | X |  |  |
| Virus, daño de equipos y archivo. |  |  | X |  |  |
| Acceso no autorizado, filtración de  Información. |  |  |  | x |  |
| Plan de acción. |  |  |  | x |  |
| Ataques, alteración de información. |  |  | X |  |  |

A continuación, se describe las puntuaciones de acuerdo a nivel de riesgos a la que está expuesta la empresa:

|  |  |  |  |
| --- | --- | --- | --- |
| **TABLA VALORACIÓN DE RIESGOS** | | | |
| **VALOR** | **TIPO DE RIESGO** | **RIESGO** | **PROTECCCIÓN**  **ACTUAL** |
|  | Fallas en los equipos | Pérdida de equipos e  información | No posee |
| Capacitación al personal | Daño de archivos por Procesos  inadecuados. | No posee |
| Acceso no autorizado, filtración  de información | Filtrado de datos por terceros o personal  interno. | No posee |
| Plan de acción | Tiempo de respuesta ante amenazas. | No posee |
| **MEDIO:** | Robo Común | Pérdida de equipos e información | * Se cierran las puertas y ventanas después fuera del horario de trabajo. * Cuenta con cámaras de video y vigilancia. |
| Ataques, alteración de  Información. | Perdida de información y disponibilidad de los sistemas. | Ninguna |
| Virus y daño de archivos | Pérdida o deterioro de la información. | - Eset con licencia |
| **BAJO:** | Incendio | Deterioro de equipos  y pérdida de información | Seguridad contra incendios adecuada. |
| Vandalismo, daño de equipos  y archivos. | Daño de equipos y  pérdida de información | Cuenta con vigilancia. |

# POLÍTICAS DE SEGURIDAD INFORMÁTICA

Se proponen con el objetivo de garantizar la protección de los principales bienes informáticos y la información contenida en ellas. A fin de informar y capacitar a toda la empresa en temas de seguridad de la información.

## Responsables

Se establece la conformación del Comité de Gestión de Seguridad de la Información, que acompañe y haga cumplir el plan de seguridad informática en función de los objetivos planteados.

Los cuales debe de estar presididos por:

|  |  |  |
| --- | --- | --- |
| **CONFORMACIÓN DEL COMITÉ DE GESTIÓN DE LA SEGURIDAD DE LA**  **INFORMACIÓN** | | |
| **Área** | **Encargado** | **Funciones** |
| **Dirección** | Titular de la Empresa | * Supervisar los incidentes sobre la seguridad. * Aprobar las iniciativas para incrementar la seguridad de la infraestructura informática. * Promover la difusión y apoyo a la seguridad de los   Activos informáticos de la empresa. |
| **Gerencia de Administración y Finanzas** | Gerente de administración y finanzas. | * Gestionar los recursos financieros para la implementación de la infraestructura informática. * Coordinar continuamente con la Dirección de Tecnología sobre la implementación y mejoras en aspecto tecnológico. |
| **Dirección de Tecnología** | Director de la Información. | * Promover la difusión y apoyo a la seguridad informática en la empresa. * Monitorear los posibles riesgos que afecten la seguridad de la información * Evaluar y coordinar la implementación de controles   específicos de seguridad informática. |
| **Asesoría Jurídica** | Jefe de la Oficina de Asesoría Jurídica | * Encargado de dar el visto legal al plan de seguridad informática, si se rige acorde a las normas y leyes de nuestra nación. * Dictaminar las normativas para cumplir y hacer cumplir por todo el personal de la empresa. |

# Medidas y procedimientos de protección Física

1. **Áreas**
   * El control de acceso y cierre de las oficinas, al terminar la jornada laboral queden correctamente cerradas. Aquellas donde se maneje información clasificada, los trabajadores de estas áreas deberán extremar las medidas de seguridad.
   * El personal autorizado tendrá visible o disponible en todo momento su identificación oficial otorgado por la empresa.
   * Los visitantes serán escoltados en todo momento por personal designado para esas funciones, quien será responsable de que el visitante tenga una conducta adecuada y aceptable.
   * La empresa debe contar con medidas de protección en caso de ocurrencia de algún siniestro tales como incendios, tormentas eléctricas, entre otras, para poder controlarlas en caso llegarán a ocurrir.
   * Cuando suscite algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa a un equipo tecnológico se deberá reportar de forma inmediata a la Dirección de Tecnología.
   * El personal de la SGTI deberá mantener un comportamiento adecuado, orientado al cuidado de los bienes tecnológicos y la información de la empresa.
   * El personal deberá tener especial cuidado con la infraestructura red instalada en las diferentes oficinas (cableado estructurado, conectores, etc.).
2. **Personal**
   * Los usuarios que hagan uso de las tecnologías informáticas son responsables de la protección de la información que utilicen o provoquen en el transcurso del desarrollo de sus labores, lo cual incluye:
     + Protección de acceso a sus computadoras.
     + Los usuarios deben tener acceso sólo a los recursos que necesitan en el cumplimiento de su labor diaria, implementándose mediante la definición del equipamiento, aplicaciones a utilizar mediante los privilegios y derechos de acceso a los activos de información que se le otorgue.
     + Se empleará las tecnologías informáticas y los servicios asociados con fines estrictamente de trabajo.
     + Todo hardware traído a la empresa se le aplicará un bloqueo. El Responsable de Seguridad Informática será el encargado de habilitarlos.
     + Los jefes de áreas y usuarios que hagan uso de las tecnologías informáticas las protegerán contra posibles hurtos, así como del robo de la información que contengan.
     + El movimiento del equipamiento informático debe ser aprobado por el responsable de seguridad informática.
     + La Dirección de Tecnología es la encargada de validar y realizar las configuraciones a los equipos informáticos; para su posterior distribución a las distintas áreas de la empresa.
     + La Dirección de Tecnología es la única encargada de dar soporte y mantenimiento a los equipos informáticos de las distintas áreas administrativas.
3. **Dispositivos externos.**
   * Una vez que un dispositivo informático haya llegado el final de su vida útil, se debe destruir el soporte de una manera adecuada, para evitar que alguien pueda obtener la información que éste almacena. Para garantizar que nadie acceda a la información. Deberá ser entregado a la Dirección de Tecnología, la cual entrega los dispositivos a una empresa de destrucción de datos informáticos.
   * Todos los soportes de información almacenados en papel deberán ser destruidos por una trituradora de papel.
   * Queda prohibido el uso de usb, discos duros externos, y otros dispositivos de almacenamiento en las áreas donde se cuente con información confidencial.

# Medidas y procedimientos de protección lógicas

1. **Identificación de usuarios.**
   * Crear credenciales de identificación de acceso (usuario y contraseña) en el servicio de directorio para acceder a la red y al correo electrónico institucional.
   * Las cuentas y claves de acceso de los servicios de internet y correo institucional son personales y confidenciales y se rigen por las políticas de contraseñas definidas en esta propuesta, para evitar el acceso a personas no autorizadas.
   * En caso de que el usuario crea que su contraseña ha sido descubierta o no lo recuerda deberá informar lo más pronto posible a la Dirección de Informática, para la asignación de una contraseña temporal.
   * El personal tiene la obligación de usar los servicios informáticos exclusivamente con fines laborales.
2. **Autentificación de usuarios.**
   * El identificador y la contraseña corresponde al medio normal de autenticación. La contraseña deberá tener al menos 8 caracteres, incluir al menos 2 numéricos y 2 alfabéticos. Se deberá cambiar de contraseña cada mes si así lo corresponde.
   * Control de acceso con huella digital. Todo personal de trabajo de la empresa deberá registrar su entrada y salida del área donde trabaja utilizando su huella dactilar, para evitar el acceso a personas no autorizadas.
3. **Control de acceso a los activos y recursos.**
   * Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. Se usará para la asignación de las credenciales de accesos a los diferentes sistemas, un formulario con el nombre del sistema, nombre usuario, contraseña temporal y la asignación de derechos al sistema y/o los servicios.
   * Se controlará e identificará los equipos conectados a su red.
   * Se utilizarán dispositivos de seguridad “firewalls”, para controlar el acceso de una red a otra.
4. **Integridad de los archivos y datos.**
   * Los usuarios notificarán sobre cualquier incidente que detecten que afecte o pueda afectar a la seguridad de los datos, o por sospecha de uso indebido del acceso autorizado por otras personas.
   * El acceso a todo tipo de datos en todas las computadoras está restringido en dependencia de los permisos que tiene asignado cada usuario.
   * Las contraseñas de los usuarios son almacenadas de forma encriptada y deben cambiarse con periodicidad (al menos cada 6 meses).
   * Las computadoras deben contar con un Antivirus actualizados.
   * EI usuario se abstendrá de enviar, vía correo electrónico, archivos que excedan la capacidad de la cuota asignada.
   * Los usuarios que utilizan documentos con información “Confidencial” o “Restringida” deben asegurarse de:
     + Almacenarlos en lugares adecuados.
     + Evitar que usuarios no autorizados accedan a dichos documentos.
     + Destruir los documentos si luego de su utilización dejan de ser necesarios.
   * Aquellos usuarios que manejen activos de información de carácter confidencial en sus equipos asignados deberán tomar los resguardos necesarios para que dicha información no sea filtrada a terceros en caso de pérdida del equipo.
5. **programas malignos**
   * El servicio de protección de antivirus debe estar siempre actualizado y controlado por el Área de Informática.
   * Es obligatorio la desinfección de los dispositivos externos antes de su uso en las estaciones de trabajo, se debe tener en cuenta que el uso de los dispositivos informáticos solo debe ser utilizadas por personas autorizadas y responsables.
   * Evitar en la medida de lo posible el uso de memorias USB. En lugar de esto, se utilizará carpetas departamentales con control de acceso lógico basado en perfiles y puestos.
   * Se prohíbe el acceso, descarga o transmisión de material cuyo origen no sea constatado como seguro o de aquél que se desconozca su confiabilidad.
   * El personal de Informática, será el encargado de efectuar la descontaminación de los ordenadores ante la aparición de programas malignos.
6. **Respaldo de información**
   * El comité de seguridad de la información debe establecer una periodicidad de cada tipo de backup.
   * Se debe contar de manera obligatoria con un registro de los Backups.
   * Debe garantizarse la disponibilidad y preservación de las Copias de Seguridad.
7. **Accesos remotos.**
   * Toda herramienta de acceso remoto a servidores y equipos de cómputo debe ser autorizada por el Área de Sistemas & T.I. e instalada por el ingeniero de Soporte designado.
   * El acceso remoto a los equipos de cómputo será autorizado por el Área de Sistemas & T.I., previa solicitud por parte del responsable de cada Área, garantizando la confidencialidad de la información de cada usuario.
8. **Auditoria y reportes**
   * Debe existir un protocolo de configuración, implementación, gestión, respaldo y recuperación de auditoría, Logs transaccionales y/o registros auditables.
   * El acceso a las pistas de Auditoría debe ser de carácter restringido a los Usuarios, solo el Área de Tecnología debe tener acceso a ellas.
   * El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones. Estos registros deben incluir lo siguiente:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | | | | | | | | | |
| Fecha de notificación: | | | | | | | | Hora de notificación: | | | | | | |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | | | | | | | | | | | | | |
| Apellido y Nombres: | | | | | | | | | | | | | | |
| Sede: | | | | | | | Área / Dependencia: | | | | | | | |
| Correo electrónico: | | | | | | |  | | | | | | | |
| Teléfono: | | Interno: | | | | | Teléfono particular: | | | | | | | |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | | | | | | | | | | | |
| Fecha en que observó el incidente: | | | | | | | Hora en que observó el incidente: | | | | | | |
| Marque con una cruz todas las opciones que considere aplicables. | | | | | | | | | | | | | |
|  | Uso indebido de información crítica. | | | | | |  | | Fraude o phishing. | | | | |
|  | Uso prohibido de un recurso informático o de red de la empresa | | | | | |  | | Modificación no autorizada de un sitio o página web de la empresa. | | | | |
|
|  | Divulgación no autorizada de información personal. | | | | | |  | | Eliminación insegura de información. | | | | |
|  | Intrusión física. | | | | | |  | | Modificación o eliminación no autorizada de datos. | | | | |
|  | Destrucción no autorizada de información. | | | | | |  | | Anomalía o vulnerabilidad técnica de software. | | | | |
|  | Robo o pérdida de información. | | | | | |  | | Amenaza o acoso por medio electrónico. | | | | |
|  | Interrupción prolongada en un sistema o servicio de red. | | | | | |  | | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) | | | | |
|
|  | Modificación, instalación o eliminación no autorizada de software. | | | | | |  | | Robo o pérdida de un recurso informático de la Empresa | | | | |
|
|  | Acceso o intento de acceso no autorizado a un sistema informático. | | | | | |  | | Otro no contemplado. Describa: | | | | |
|
| Describa brevemente cómo detectó el incidente: | | | | | | | | | | | | | | |
| El incidente aún está en progreso: | | | [ | ] SI | [ | ] NO | | | | | | | | |
| Tiempo estimado de duración del incidente: | | | | | | | | | | | | | | |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: | | | | | | | | | | | | | | |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | | | | | | | | | | |
| Sistema, computadora o red afectada: | | | | | | | | | | | | | |
| Localización física: | | | | | | | | | | | | | |
| Describa brevemente la información contenida en el sistema / computadora: | | | | | | | | | | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? | | | | | | | | | |  | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red de la empresa | | | | | | | | | |  | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? | | | | | | | | | |  | SI |  | NO |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente: Si el incidente: •se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. •se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. •se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de Tecnologia y reenvíe el mensaje como adjunto a la dirección seguridadinformatica@fctech.ar |

# Plan de Contingencia

Es de vital importancia ya que se establece con el fin de garantizar la continuidad de los servicios ante cualquier desastre que pueda ocurrir. Por tal Motivo se plantean estas medidas, de acuerdo al resultado del análisis de riesgos realizado anteriormente:

|  |  |
| --- | --- |
| **1. INCENDIO** | **Objetivo**: Proteger del fuego la información de la institución que se encuentra alojada en las estaciones de trabajo que podrían dañarla de manera parcial o total. |
| **QUE HACER:** | 1. Utilizar los extintores instalados para sofocar el incendio. 2. Apagar los principales dispositivos de la SGTI, puesto que es el soporte principal de la infraestructura tecnológica. 3. Desconectar las llaves de alimentación eléctrica. 4. Llamar a los bomberos. |
| **RESPONSABLE:** | Dirección de Tecnología y el personal de la institución - Personal de Seguridad |

|  |  |
| --- | --- |
| **2. FALLAS EN LOS EQUIPOS, DAÑOS DE ARCHIVOS.** | **Objetivo**: Proteger los bienes informáticos, de posibles daños físicos y lógicos, que atenten contra el buen funcionamiento de las mismas. |
| **QUE HACER:** | 1. Reportar la falla al Personal de Soporte de la Dirección de Tecnología. 2. El personal de informática revisara el equipo para diagnosticar y proceder a reparar el desperfecto. 3. Revisar y corregir error. |
| **RESPONSABLE:** | Dirección de Tecnología |

|  |  |
| --- | --- |
| **3. EQUIVOCACIONES, DAÑOS DE RCHIVOS.** | **Objetivo**: Proteger de la información de la empresa, que se encuentra alojada en las estaciones de trabajo, de errores humanos que podrían dañarla de manera parcial o total. |
| **QUE HACER:** | 1. Reportar el problema a la Dirección de Tecnología, para que se proceda a corregir el error. 2. Realizar Copias de Seguridad de los archivos, para salvaguardar la información. 3. Solicitar la evaluación del equipo y dispositivo donde se alojó el archivo corrupto para descartar fallas a nivel software y hardware que lo hayan provocado. |
| **RESPONSABLE:** | Dirección de Tecnología |

|  |  |
| --- | --- |
| **4. ACCESO NO AUTORIZADO, FILTRACIÓN DE****INFORMACIÓN.** | **Objetivo**: Mejorara el nivel de control de acceso hacia la entidad y las oficinas administrativas, para salvaguardar la información y bienes de la empresa. |
| **QUE HACER:** | 1. Cambiar inmediatamente contraseñas de acceso de administradores y de base de datos. 2. Verificar la información filtrada 3. Realizar el respaldo de la información. 4. Chequear el tráfico de la red para detectar variaciones que pueden ser síntoma de mal uso de la misma. 5. Reportar al Director de tecnología. |
| **RESPONSABLE:** | Dirección de Tecnología |

|  |  |
| --- | --- |
| **5. VIRUS Y DAÑO DE ARCHIVOS** | **Objetivo**: Proteger los equipos computacionales y la red institucional de posibles infecciones por software malicioso. |
| **QUE HACER:** | 1. Al detectar en una estación de trabajo indicios de ataques detener la actividad que se esté realizando, desconectarla de la red y avisar al personal informático. 2. Efectuar la limpieza de las computadoras ante la aparición de programas maliciosos. 3. Se debe de realizar la correcta actualización del Software Antivirus en el Servidor principal. |
| **RESPONSABLE:** | Dirección de Tecnología |

Después de ocurrida la contingencia es necesario realizar las actividades como:

## Evaluación de daños

Después de la contingencia, se deberá evaluar la magnitud del daño que se ha producido, que fueron afectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

## Contención y mitigación

Identificado el incidente, hay que contenerlo y mitigar sus efectos usando la información obtenida anteriormente. Para ello es esencial definir la extensión, el tipo de equipos afectados y buscar las características comunes para poder aislar el incidente en función de esos patrones.

La ejecución de las actividades enmarcadas en las políticas establecidas, deberán ser realizadas por los equipos operativos pre establecidos por el comité de gestión de la seguridad de la información.

La restauración deberá intentarse en primer lugar con los recursos afectados y de acuerdo a evaluaciones posteriores, se deberá volver a adquirir los recursos, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio que brinda la empresa.

## Evaluación y resultados

Una vez concluida las labores de recuperación posteriores a la contingencia, se realizará una evaluación de los resultados del plan de contingencia las mismas que nos servirán para aplicar mejoras al plan de seguridad informática y fortalecer las políticas de seguridad hasta dejar de lado el plan de contingencia.

# Recomendaciones:

* + Es de carácter primordial capacitar al personal de Informática para que, puedan mantener el correcto funcionamiento de la infraestructura y los servicios que brinda la oficina y no existan inconvenientes en el uso de las aplicaciones de trabajo cotidiano.
  + Capacitar al personal que trabaja en la empresa, sobre el adecuado uso de los recursos informáticos.
  + Se recomienda licenciar las aplicaciones que son de usos administrativos.
  + Se recomienda la instalación de equipos firewall adecuados.
  + Se recomienda la implementación del certificado digital de seguridad del portal web institucional (Protocolo SSL).
  + Recomendamos además la implementación en una primera etapa, de nuevas infraestructuras necesarias y consideradas de inmediata atención, que son:
    - Adquisición de licencias de un sistema de seguridad antimalware, herramientas de administración de it y mesa de ayuda.
    - Contar con un sistema de seguridad antimalware que incluya contención, veredicto de malware en la nube, herramientas de administración de TI y mesa de ayuda, que asegure la protección de los equipos de cómputo, servidores y dispositivos móviles para que disminuya el riesgo de vulnerabilidades que pueda tener la infraestructura de la red causada por malware. De esta manera, evitar que los servicios y funciones que se presta a todos los usuarios no se vea afectados.
    - También, el sistema debe incluir herramientas de administración de TI que permita tener el control de aplicaciones, control de dispositivos, control de acceso remoto, inventario de hardware, inventario de software, instalación de aplicaciones de forma masiva, control de recursos de hardware, sistemas de alertas y eventos, control de cuentas de usuarios, entre otras funciones y permita realizar el mantenimiento de pc y servidores de forma remota y centralizada. Por último, debe incluir un sistema de mesa de ayuda (generación de tickets atención e incidencias) que permita tener documentado el servicio del soporte técnico brindado por la oficina de informática y el personal de soporte técnico con la finalidad de mejorar los servicios que la oficina de informática presta a los usuarios de la organización.