Política de Seguridad de la Información
Sincrón Diseño Electrónico SAS

INTRODUCCIÓN

SINCRÓN DISEÑO ELECTRÓNICO SAS identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por Sincrón SAS. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de SINCRÓN SAS y definen lo que está permitido y lo que está prohibido y los procedimientos y herramientas necesarias, para garantizar el buen uso de los recursos tecnológicos que la empresa SINCRÓN SAS pone a disposición de sus funcionarios para el cumplimiento de sus funciones.

La seguridad de la información es una prioridad para SINCRÓN SAS y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia de cada una de estas políticas.

CONTENIDO

1. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de SINCRÓN SAS, con el fin de regular la gestión de la seguridad de la información al interior de la compañía.

2. ALCANCE

Esta Política de seguridad es elaborada de acuerdo al análisis de riesgos y vulnerabilidades que presenta actualmente la empresa SINCRÓN SAS. Sin embargo puede servir de base para otras empresas que lo requieran de acuerdo a sus necesidades

Es aplicable para todos los funcionarios de la empresa SINCRÓN SAS ya sea personal de planta, contratistas, funcionarios de empresas prestadoras de servicios entre otros, quienes por sus funciones tengan un equipo de cómputo ya sea asignado por la empresa o personal y que esté conectado a la red de la empresa.

Abarca también todos los equipos de cómputo perteneciente a empresas subcontratadas y sus usuarios, siempre que estos estén conectados a la red de cualquier forma de conexión, local, remota, física, lógica y/o que hagan uso de los recursos tecnológicos de la empresa SINCRÓN SAS.

Comprende los siguientes aspectos:

- Control de acceso (aplicaciones, base de datos, área del Centro de Cómputo).
- Resguardo de la Información.
- Clasificación y control de activos.
- Gestión de las redes.
- Gestión de la continuidad del negocio.
- Seguridad de la Información en los puestos de trabajo.
- Controles de Cambios.

- Protección contra intrusión en software en los sistemas de información.
- Monitoreo de la seguridad.
- Identificación y autenticación.
- Utilización de recursos de seguridad.
- Comunicaciones.
- Privacidad.

3. GLOSARIO

Bases de Datos. Una **base de datos** es un "almacén" que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente

Confiabilidad: Está determinada por el posible daño, como resultado de una operación del sistema de información realizada en forma incorrecta, incompleta, impropia o inoportuna.

Confidencialidad: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Funcionarios: Personal contratado por la empresa SINCRÓN SAS, indistintamente de estar nombrado de planta, subcontratado o en entrenamiento.

Política: Es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. También puede definirse como una manera de ejercer el poder con la intención de resolver o minimizar el choque entre los intereses encontrados que se producen dentro de una sociedad.

Red LAN: Red de Área Local (Local Área Network).

Usuario: Es aquel funcionario que tiene relación directa con los aplicativos, bases de datos, Sistemas operativos, equipos de cómputo o de comunicaciones de la empresa.

Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria, es una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.
Contraseña o Clave: Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso. Las

claves suelen tener limitaciones en sus caracteres (no aceptan algunos) y su longitud.

Seguridad de la información: Es un término que hace referencia a la seguridad de activos de forma general, incluyendo la seguridad informática, la seguridad TIC y la seguridad de los datos.

Seguridad informática: "Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable."(Aguilera López, Purificación, 2010).

Seguridad Pasiva: Son el conjunto de medidas o estrategias que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema.

Seguridad Activa: Son todas las acciones enfocadas a prevenir y detectar los riesgos para la seguridad de la información.

Seguridad Física: Son el conjunto de métodos y herramientas usadas para proteger el sistema informático, mediante el uso barreras y mecanismos de control a nivel del Hardware

Seguridad Lógica: Su enfoque se fundamenta en las estrategias encaminadas a proteger los programas (Software), de un sistema informático.

Mecanismos de seguridad: Todo aquello de naturaleza hardware y software que se utiliza para crear, reforzar y mantener la seguridad informática. Se clasifican en:
Preventivos: Actúan antes de que se produzcan ataques. Su misión es evitarlos.

Detectores: Actúan cuando el ataque se ha producido y antes que cause daños en el sistema.

Correctores: Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

4. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

En SINCRÓN SAS la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, SINCRÓN SAS implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del Sincrón SAS, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política Global de Seguridad de la Información del Sincrón SAS se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la empresa. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

SINCRÓN SAS, podrá modificar la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

5. COMPROMISO DE LA DIRECCION

La Gerencia de Sincrón Diseño Electrónico SAS, aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Alta Dirección de la empresa demuestran su compromiso a través de:

La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
La promoción activa de una cultura de seguridad.
Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
La verificación del cumplimiento de las políticas aquí mencionadas.

6. POLITICAS DE SEGURIDAD DE SINCRÓN

Principio Básico y Fundamental:

"**L o que no está permitido en esta política de seguridad, está expresamente prohibido**."

A. POLITICAS DE SEGURIDAD LOGICA.

I. CONTROLES DE ACCESO A EQUIPOS DE CÓMPUTO, SISTEMAS DE INFORMACIÓN, BASES DE DATOS Y A LA RED.

1. Será responsabilidad de la dirección de la empresa SINCRÓN SAS, establecer una adecuada segregación de funciones dentro de su estructura organizacional en el departamento de informática, estas funciones deben ser asignadas de manera adecuada al personal calificado.
2. Es responsabilidad de la empresa SINCRÓN SAS, asegurar que cada funcionario tenga asignado, unos derechos de acceso a los sistemas de

información y recursos informáticos, de acuerdo a sus funciones, que permanezcan actualizados con el nivel de autorización asociado a sus funciones y le permitan desarrollar adecuadamente su trabajo.

3. Cada funcionario debe contar con una identificación única e intransferible dentro del sistema de control de accesos. La combinación de usuario y "contraseña" debe ser única.
4. Cada funcionario se hará responsable de las actividades y transacciones que se realicen con su "usuario y contraseña" ya que estos son de carácter confidencial e intransferible. Deben tener claro los aspectos legales que puede acarrear acciones negativas realizadas con su respectivo usuario.
5. Los derechos de acceso de los funcionarios a los sistemas de información y/o bases de datos de la empresa SINCRÓN SAS, deben estar acorde a sus funciones, deben ser autorizadas por la dirección de la empresa, y será evaluada y avalada por el responsable de la seguridad informática de la empresa.
6. Los derechos de acceso deben ser asignados de tal forma que no interfieran con las actividades o datos privados de otros funcionarios.

- Para la "contraseña" asignada al nombre de usuario, se deben tomar las siguientes recomendaciones:
- Las "contraseñas" de usuario deben ser alfanumérica, contener caracteres especiales y una longitud no menor a 8 caracteres, no utilizar espacios en blanco.
- La contraseña no debe revelarse bajo ninguna circunstancia.
- No se deben reutilizar contraseñas ya utilizadas.
- El nombre de usuario y la contraseña no puede ser iguales.
- No se debe utilizar contraseñas fácilmente descifrables como fecha de cumpleaños, nombres de familiares y apellidos, números de identificación, entre otros.

- Se debe prohibir el uso de contraseñas cíclicas como por ejemplo meses más del año (noviembre2015).
- Para evitar el olvido de las contraseñas y el tener que escribirlas en algún lugar por parte del usuario, estas deben ser fácilmente pronunciables.

7. Está totalmente prohibido que un funcionario autorice el uso de usuario y contraseña a otras personas.
8. Los funcionarios no podrán dejar nombres de usuario y contraseñas escritos en lugares donde puedan ser vistos o tomados por terceros.
9. Cuando se asigne un usuario por primera vez a un funcionario, se debe dar a conocer inmediatamente la política de seguridad de la empresa.
10. Cuando se asigne un usuario y contraseña por primera vez a un funcionario, el departamento de informática en el directorio activo debe establecer la regla para que el propio funcionario realice el cambio de la misma de forma inmediata.
11. Cada sistema debe contener la información necesaria para identificar cada nombre de usuario con el funcionario responsable de su uso.
12. El departamento de informática deberá establecer regla en el directorio activo para que obligatoriamente cada funcionario realice cambio de contraseña por lo menos cada 45 días.
13. El departamento de Informática deberá revisar como mínimo semestralmente los derechos de accesos asignados a los usuarios administradores de los sistemas bajo su responsabilidad grupos de privilegios (incluye personal de la propia oficina, personal técnico, auditor y cualquier otro que lo requiera), se debe verificar estos derechos están ajustados a las funciones y tareas de cada funcionario.

14. Todas las revisiones o modificaciones que se realicen sobre el directorio activo y sobre el controlador de dominio debe quedar debidamente registrado en una

bitácora de acciones.

15. Cada vez que un funcionario se ausente de la oficina por vacaciones, incapacidades, licencias y que este tiempo sobrepasen 3 días hábiles el departamento de informática previa información del departamento de talento humano deshabilitara los derechos de acceso del usuario, hasta tanto no se realice el reintegro a sus labores por parte del funcionario.
16. Los funcionarios no deben dejar desatendido el equipo de cómputo, de requerir alejarse del puesto de trabajo, el funcionario debe cerrar los aplicativos o bases de datos sobre las cuales este trabajando, y debe dejar bloqueada la sesión de trabajo.
17. La empresa debe establecer horario de trabajo sobre las bases de datos y/o aplicaciones, estos horarios deben cumplirse por lo anterior el departamento de informática debe establecer políticas de seguridad lógicas para que esto se cumpla, en caso de que algún funcionario requiera trabajar por fuera del horario, el jefe del funcionario deberá autorizarlo y responder por lo que su funcionario realice. Debe informarse al departamento de informática para la habilitación del permiso de trabajo extra horario autorizado.
18. Al terminar la relación laboral de cualquier funcionario (despido, renuncia, incapacidad, pensión, etc.), será responsabilidad del departamento de talento humano informar inmediatamente al departamento de informática para que revoque y deshabilite el usuario y los privilegios otorgados.
19. Se debe mantener en un sobre sellado y bajo la responsabilidad del Responsable del departamento de informática, un código de usuario de contingencia y su respectiva contraseña que posea todos los privilegios del Administrador de la Red, Administrador de Base Datos u otros, para ser utilizado solamente en caso de emergencia. En caso de requerir su uso debe quedar debidamente registrado. Esta contraseña debe ser actualizada mínimo cada seis meses.
20. El departamento de informática debe prohibir lógicamente las sesiones

múltiples de un usuario de red, este debe ser un privilegio exclusivo de administradores del sistema.

II. USO DE LOS EQUIPOS Y SERVICIOS.

1. El departamento de informática debe restringir el almacenamiento e instalación de juegos en los equipos de cómputo. Los funcionarios tienen prohibido almacenar juegos y utilizar los equipos de cómputo de la empresa para este tipo de actividades.

2. Los equipos de cómputo, aplicaciones, bases de datos y toda la información de la empresa no podrán utilizarse para fines personales.

3. Todos los funcionarios tienen prohibido suministrar los equipos de cómputo, aplicaciones, bases de datos y toda la información de la empresa a personas externas o sin vínculo laboral con la empresa

4. SINCRÓN SAS, podrá establecer los controles de acceso y demás medidas de seguridad que le permitan garantizar la protección de su información, aplicaciones, bases de datos y parque tecnológico como son:

    a. Restringir o derogar cualquiera de los privilegios a cualquiera de los usuarios.
    b. Inspeccionar, copiar, remover o bien alterar algún dato, programa u otro sistema que pueda ir en contra de los objetivos de la empresa.
    c. Tomar cualquier otra acción que estime necesaria para manejar y proteger sus aplicativos y bases de datos. La empresa no estará en la obligación de notificar a los usuarios.

5. Se prohíbe a todos los funcionarios el uso de aplicativos y bases de datos, información para dañar, deteriorar o alterar los activos de la empresa.

III. CONTROL DE SOFTWARE MALIGNO.

1. Con el fin de evitar daños al parque computacional, equipos activos de la red, información, aplicativos, bases de datos entre otros, el departamento de informática deberá gestionar ante la dirección, la compra de software debidamente licenciado como son, antivirus, antimalware, antispyware.
2. La dirección de la empresa, está en la obligación de atender las sugerencias del departamento de informática para obtener el mejor software para proteger su parque computacional, equipos activos de la red, información, aplicativos, bases de datos entre otros.
3. El departamento de informática deberá configurar en todos los equipos de cómputo el software adquirido para control de software maligno , de forma tal que funcione su actualización y verificación de dispositivos automáticamente, deben establecer y configurar desde el servidor todas las políticas necesarias para evitar algún tipo de daño por software maligno.
4. Los funcionarios deberán informar inmediatamente al departamento de informática, sobre cualquier novedad que observen sobre el funcionamiento o detecciones de este tipo de software de protección, no deben tomar acciones propias.
5. Se prohíbe a los funcionarios la instalación de software libre o licenciado obtenido por cualquier medio, solo se podrá contar con el software establecido por la dirección de la empresa y el departamento de informática.
6. El departamento de informática deberá configurar sobre el servidor de antivirus la restricción de uso de puertos USB, y el acceso a dispositivos USB, en todo el parque computacional, solo tendrán permisos aquellos funcionarios a quienes se les realice estudio y por la naturaleza de sus funciones lo requieran y sea de vital importancia.
7. Todos los funcionarios deben descomprimir información recibida y hacer revisión para corroborar que no son archivos contaminados, antes de abrirlos y

utilizarlos.

8. El departamento de informática debe configurar un sistema de protección contra escritura en cada equipo de cómputo y servidores con el fin de proteger sus activos en caso de que una maquina sea contaminada por un software maligno.
9. En cada mantenimiento preventivo y/o correctivo que se realice al parque computacional por el funcionario o empresa encargada de esta función, se debe verificar la instalación del software de control de software maligno, su actualización y correcto funcionamiento.
10. Los usuarios no deben tener acceso a la configuración del antivirus, solo los administradores.

IV. PROCESO DE CONTROL DE CAMBIOS.

1. En cada mantenimiento preventivo y/o correctivo que se realice al parque computacional por el funcionario o empresa encargada de esta función, se debe verificar estado y actualización de los sistemas operativos, igualmente se debe verificar que solo este instalado el software autorizado por la empresa. En caso de encontrar software no autorizado debe registrarlo en la bitácora de mantenimiento e informar inmediatamente al departamento de informática para que tomen las acciones procedimentales y legales correspondientes.

2. Se prohíbe a todos los funcionarios de la empresa el engaño a los controles de acceso establecidos en los sistemas operativos con el fin de dejar libre la opción de puertas traseras que puedan hacer daño a los activos de la empresa.

V. OPERACIÓN DEL COMPUTADOR.

1. Evitar comer y beber en el centro de cómputo e instalaciones con equipos tecnológicos.
2. Evitar beber, comer cerca de cualquier equipo que haga parte del parque

computacional, sea o no el asignado.

B. POLÍTICA DE RESPALDOS Y RECUPERACIÓN.

1. El departamento de informática deberá definir el personal autorizado y responsable para la realización de los diferentes respaldos que la empresa y sus funcionarios requieran. Este personal también debe estar en la capacidad de recuperar la información cuando sea necesario
2. Se debe establecer un modelo de archivo lógico por parte del departamento de informática de forma tal que al llegar a un equipo de cómputo y se requiera realizar el respaldo de la información, se realice a la documentación que se establece y no se genere redundancia que pueda afectar la capacidad del dispositivo de almacenamiento. (Ejemplo, establecer el nombre del proceso al que pertenece el funcionario, crear carpeta por años, luego por temas. Se debe obviar el respaldo de archivos personales de los funcionarios, este respaldo va dirigido exclusivamente a lo que concierne a la empresa.
3. En el respaldo de los datos se debe considerar tanto los datos de la aplicación (archivos, bases de datos, datos estructurados y no estructurados) como los demás elementos necesarios para asegurar la prestación de servicios, tales como el software de la aplicación (programa parámetros de operación, documentación complementaria a los procesos, sistemas operativos, software de ambiente y demás.

4. El departamento de informática debe crear un cronograma de la programación del proceso de respaldo (diario, semanal, mensual y anual), además se debe contar con procedimientos de verificación y supervisión de los procesos y del contenido de los respaldos.
5. Todos los procesos de respaldo y recuperación de información deben

proveer los elementos que evidencien (log de eventos) la ejecución del proceso, detalle del contenido de los mismos, así como deficiencias en caso de existir.

6. Los medios de respaldo deben ser protegidos de borrados accidentales a través del uso de medios físicos y lógicos de carácter preventivo (“lock” en los medios de Backup, otros).
7. Los medios de respaldo se deben etiquetar, las etiquetas deben tener información de su contenido, nombre, fecha del respaldo y funcionario que lo realizó.
8. Los respaldos de datos y demás elementos necesarios, deben estar almacenados en sitios que dispongan de condiciones de acceso restringido y de medio ambiente apropiado a los medios utilizados, así como para hacer frente con éxito a eventos contingentes como incendios, inundaciones u otros.
9. Antes de proceder a la restauración de datos sensibles o críticos a partir de un respaldo se debe realizar una copia de los mismos para minimizar efectos de corrupción o daños de los datos originalmente respaldados.
10. Se debe generar una copia de todos los respaldos, los cuales se custodiarán en un sitio alterno, que cumpla con las características y protección ambiental similares al sitio principal. La proximidad entre el sitio principal y el alterno se debe contemplar dentro de los parámetros que se establezcan en el convenio de salvaguarda y custodia de información. Se recomienda disponer al menos de dos vías de acceso distintas.
11. Se deben tomar las medidas de seguridad necesarias para el traslado de los medios de respaldo al sitio alterno, a fin de garantizar no solo que llegarán a su destino sino la integridad de los medios.
12. Como mínimo semestralmente se debe verificar la validez de los respaldos custodiados en el sitio principal y en sitio alterno. Se debe verificar la condición de los medios de almacenamiento y si los datos pueden ser

restaurados oportuna y confiablemente.

13. A los equipos y los medios usados para el respaldo se les debe realizar periódicamente mantenimiento preventivo por parte del personal encargado de esta función. Se debe asegurar correcto funcionamiento de los mismos.

C. SEGURIDAD DE REDES LAN- LAN EXTENDIDA.

1. El responsable del departamento de informática de la empresa SINCRÓN SAS, debe nombrar un responsable para la administración de la red LAN - WIFI, cuyas funciones y tareas deben estar claramente definidas y delimitadas.
2. Todo el parque computacional (computadoras, estaciones de trabajo, estaciones gráficas, servidores y equipo accesorio, dispositivos móviles, tabletas, Smartphone), que esté o sea conectado a la Red de la empresa, o aquel que en forma autónoma se tenga y que sea propiedad de la empresa, o que use la red de datos de la empresa debe sujetarse a las normas y parámetros de instalación y configuración que emita la empresa SINCRÓN SAS.
3. El departamento de informática debe contar con un inventario actualizado de los activos informáticos propiedad de la empresa y también inventario de los equipos que no pertenezcan a la empresa pero estén conectados a la red, con la información del funcionario responsable, software instalado, permisos de usuario y todo lo que corresponda a cada elemento.
4. El departamento de informática coordinará con el funcionario o la empresa encargada del mantenimiento preventivo y correctivo del parque computacional, la realización de estas tareas, así como la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir los procesos internos respectivos y relacionar dichas tareas en el sistema de información destinado para ello.

5. El departamento de informática debe proteger con medios físicos (tales como candado, fajas, etiquetas u otros) aquellos equipos o sus componentes que por su valor o exposición pueden estar sujetos a pérdidas o sustracción.
6. La adquisición de hardware y software sebe ser gestionada a través del departamento de informática en conjunto con el departamento administrativo bajo las directrices y normativas técnicas de la empresa.
7. Todo el parque computacional debe ser objeto de mantenimiento preventivo y/o correctivo, se debe programar anualmente un cronograma por el departamento de informática.
8. En los equipos de la empresa, únicamente se debe instalar el software debidamente autorizado por el departamento de informática y para el que se disponga de las licencias de uso respectivo.
9. Está prohibido el uso del software y recursos informáticos propiedad de la empresa SINCRÓN SAS, para fines ajenos a las actividades propias de la empresa.
10. El funcionario o la empresa encargada del mantenimiento preventivo y correctivo del parque computacional serán responsable del soporte y buen funcionamiento de los equipos de cómputo de la red de la empresa SINCRÓN SAS, bajo la supervisión del responsable departamento de informática, según los términos establecidos en la contratación del servicio y deben asegurar que las condiciones de medio ambiente en que operan éstos se ajustan a las establecidas por departamento de informática.
11. Se debe contar con documentación actualizada sobre los componentes y organización de las redes de la empresa SINCRÓN SAS y de los recursos asociados a ésta, entre otros: enlaces y diapositivas de conexión físicas, protocolos de comunicaciones y direcciones IP, segmentaciones de la LAN extendida y canales de comunicación.
12. Los requerimientos para la instalación y actualización de redes deben ser

formalizados y controlados adecuadamente, asegurando que su ejecución no interfiera con la operación normal de los servicios.

13. El departamento de informática debe contar con Sistema de detección de intrusos instalados y correctamente configurados para evitar vulnerabilidad en la red y en sus equipos.
14. El departamento de informática debe contar con Firewall instalados y correctamente configurados para evitar vulnerabilidades de la red.
15. El acceso a la red interna debe ser a través de un mecanismo de autenticación.
16. El área de TI debe implementar los mecanismos necesarios para bloquear, enrutar o filtrar el tráfico para evitar acceso o información no autorizada hacia la red interna o de la red interna para el exterior.
17. Se debe registrar todo acceso a los dispositivos de la red mediante archivos de Log y se revisaran en un tiempo de 48 horas.

D. POLÍTICAS DE ACCESO Y USO DE WIFI.

1. La administración de los recursos de tecnologías de la información y las comunicaciones es importante para el cumplimiento y desarrollo de labores en la empresa SINCRÓN SAS.
2. Las redes inalámbricas requieren de un alto grado de responsabilidad por parte de los usuarios de la red para aprovechar y maximizar los beneficios de la tecnología, brindando cobertura de red inalámbrica y un sistema de comunicaciones seguro en las edificaciones de la entidad.
3. El departamento de informática deberá difundir las políticas entre los usuarios de los recursos y bienes informáticos. A continuación se definen las políticas relacionadas con la red inalámbrica WLAN:

- El departamento de informática establecerá los procedimientos para la instalación, administración y configuración de la red inalámbrica de la

entidad, con el fin de mantener la integridad, seguridad de la información así como la seguridad de la infraestructura de red LAN y WLAN.

- Los equipos y antenas inalámbricas única y exclusivamente deberán ser instalados por personal del departamento de informática o por personal avalado por el departamento de informática, así como su supervisión y monitorización de uso.
- El departamento de informática debe evitar el mal uso de la red inalámbrica de la empresa SINCRÓN SAS, así como el acceso a sistemas o aplicaciones no autorizadas (Redes Sociales, reproducción de videos, juegos en línea, descarga de aplicativos) que afectan el desempeño de la red inalámbrica diseñada y destinada con fines netamente laborales.
- El departamento de informática monitoreara las páginas visitadas, y las mismas serán restringidas a través de los perfiles de navegación definidos en esta política.
- El departamento de informática debe regular y controlar la instalación de equipos inalámbricos externos a la red de la empresa como equipos móviles de comunicación para prevenir la interferencia con otros usuarios que utilicen el mismo espectro de frecuencias.
- El departamento de informática restringirá la propagación de SSID de dispositivos de anclaje, como modem 3G, 4G, y zonas de anclaje de celulares Smartphone.
- El departamento de informática debe monitorear y generar reportes de tráfico de los usuarios de la red Inalámbrica de la empresa SINCRÓN SAS.

E. POLÍTICAS DE ACCESO Y USO DE INTERNET.

1. Es responsabilidad de cada usuario el uso prudente de las tecnologías como el internet, que la empresa coloca a su disposición.

2. Se prohíbe a todos los funcionarios el acceso a sitios de Internet que no tengan relación alguna con los objetivos de la empresa, como son: pornografía, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación al uso de buenas prácticas y sanitización de la red.
3. No se autoriza a los funcionarios acceder a sitios para el establecimiento de charlas, salvo que tengan relación alguna con las funciones que desempeña, para ello el departamento de informática hará las respectivas configuraciones.
4. Sólo funcionarios con previa autorización podrán “descargar” información desde Internet, esto se hará bajo la supervisión y monitoreo del departamento de informática.
5. Toda información descargada de Internet debe estar relacionada con los objetivos de la empresa y las funciones que lleva a cabo el usuario.

6. Todos los archivos obtenidos desde Internet deben ser revisados para detección de virus previo a ser descargados en cualquier computador.
7. Ningún documento, información, software, no puede ser transferida a terceros sin autorización y un compromiso de confidencialidad entre la empresa y terceros.
8. El tiempo de acceso a Internet no debe interferir ni distraer a los usuarios de sus funciones normales.
9. Toda información que transite por la red de la empresa se considera propiedad de la empresa SINCRÓN SAS.
10. La información transmitida, procesada producto de las funciones del personal y que concierne a SINCRÓN SAS, o a sus funcionarios, no podrá ser interceptada o divulgada bajo ninguna circunstancia, por ningún usuario interno de la red de la empresa, salvo en aquellos casos que los organismos de seguridad establezcan bajo órdenes judiciales.

F. POLITICA SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

Para acceder a áreas restringidas se debe realizar la notificación para obtener la autorización y de esta manera proteger la información y bienes informáticos.

I. PROTECCIÓN DE LA INFORMACIÓN Y DE LOS BIENES INFORMÁTICOS

1. Todo funcionario debe informar cuando detecte riesgo o amenaza a equipos de cómputo o comunicaciones.
2. Todo funcionario debe proteger las unidades de almacenamiento a su cargo.
3. Todo funcionario tiene como responsabilidad de evitar fugas de información de la empresa que se encuentre almacenada en los dispositivos que tenga a su cargo.

II. CONTROL DE ACCESO FÍSICO

1. Toda persona que ingrese SINCRON SAS debe registrar en la entrada los dispositivos que traiga bien sea de computo, almacenamiento o comunicaciones y deberá reportarlo su salida al momento de retirarse de la empresa.
2. Todo computador, unidad de almacenamiento o equipo de comunicaciones debe tener permiso por el área de TI para poder ser retirado de la empresa SINCRON SAS.

III. SEGURIDAD EN ÁREAS DE TRABAJO

1. El centro de cómputo de SINCRÓN SAS deberá estar restringido y solo puede ingresar personal autorizado.

IV. PROTECCIÓN O UBICACIÓN DE EQUIPOS

1. Los usuarios de SINCRÓN SAS no debe mover los equipos de cómputo o comunicaciones, igualmente se prohíbe la instalación o desinstalación de dispositivos o el retiro de sellos de los mismos sin la autorización del área de TI.

2. El equipo asignado será para uso exclusivo de las actividades de los usuarios de SINCRÓN SAS.
3. No se debe ingerir alimentos mientras se utilizan los dispositivos.

V. MANTENIMIENTO DE EQUIPOS

1. Solo las personas autorizadas deben realizar mantenimiento a los equipos de cómputo.
2. Cuando se lleve a mantenimiento el equipo de cómputo se debe realizar backup de toda la información y eliminar la información sensible del PC.

G. POLITICAS ADICIONALES

I. CONEXIÓN A INTERNET

1. La conexión a internet es restringida de acuerdo a los parámetros establecidos por la organización.
2. Se deben conectar sólo los dispositivos autorizados.
3. Cada usuario debe responder por la navegación realizada desde su computador.
4. En caso de realizar transacciones personales, el usuario se hará responsable de ellas, aunque no se deberían realizar ya que los equipos de cómputo son solamente para funciones laborales.
5. No utilizar el internet para descargar programas y canciones.
6. El uso de mensajería instantánea, correos, foros, entre otros debe ser solamente para actividades relacionadas con la empresa.

II. CORREO ELECTRÓNICO

1. El uso del correo electrónico debe ser solamente relacionado a actividades laborales.
2. No utilizar el correo con fines personales.

3. En caso de sospechar de algún correo, informarlo al personal encargado de la seguridad informática.
4. Los correos corporativos deben llevar la firma del remitente.
5. Verificar que los archivos adjuntos no estén infectados.
6. Evitar participar en cadenas de oración, y reenvió de correos, ya que estos son factores decisivos para que un atacante pueda vulnerar la red de la empresa.
7. No se debe ingresar al correo de otros usuarios y manipular la información.
8. Las cuentas de correo deben estar previstas de claves.
9. Cada usuario se hará responsable el uso que le dé a su cuenta de correo.
10. Los mensajes enviados por el correo corporativo son de propiedad de SINCRÓN SAS por lo tanto la comunicación debe ser privada y segura.
11. Se prohíbe falsificar, esconder, eliminar o reemplazar la identidad de un usuario de correo.

III. USUARIOS Y CONTRASEÑAS

1. Para el ingreso a los sistemas de información cada usuario debe contar con un nombre de usuario y contraseña.
2. Las claves se deben cambiar cada 30 días, sin permitir que se repitan
3. El número máximo de intentos para el ingreso será de cinco veces, en caso de completar todos los intentos, el sistema bloqueara el ingreso, siendo necesario adquirir una nueva clave.
4. Las contraseñas serán asignadas por el personal encargado de la seguridad informática, permitiendo el cambio de contraseña de forma inmediata, evitando así que otras personas, incluso el encargado de seguridad pueda tenerlas, su almacenamiento debe ser cifrado.

5. Lac contraseñas deben contener máximo ocho caracteres alfanuméricos.

IV. SOFTWARE

1. Se debe utilizar únicamente software legal
2. Queda prohibido la reproducción de programas como software ofimático, sistemas operativos entre otros.
3. Informar sobre las actualizaciones de los programas antivirus.
4. Chequeo de medios extraíbles autorizados para su uso por medio de antivirus.
5. Queda prohibido descargar programas y música.

V. PROPIEDAD INTELECTUAL

1. Se debe respetar la política de propiedad intelectual, por lo cual no se deben instalar en los equipos de cómputo. aplicaciones que carezcan de licencias adquiridas de manera formal.
2. Se prohíbe la duplicación de material que carezca de licencia original.

H. SANCIONES.

1. Cualquier violación a la política de Seguridad informática de SINCRÓN SAS deberá ser sancionada de acuerdo al Reglamento de Trabajo, igualmente se tendrán en cuenta las normas, leyes y estatutos de la ley Colombiana como lo es *La Ley 1273 de 2009,* entre otras.
2. Las sanciones van desde una llamada de atención al funcionario infractor hasta el despido de la empresa supeditado a que se puedan realizar demandas penales dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.
3. El departamento de informática debe elaborar un informe preliminar a la Dirección de SINCRÓN SAS, con copia a quien corresponda con

las infracciones a la seguridad correspondiente, con el fin de que se tomen las acciones normativas que correspondan a quienes violen las disposiciones en materia de informática de la empresa.

4. Todas las acciones en las que se comprometa la seguridad de la Red de SINCRÓN SAS y que no estén previstas en esta política, deberán ser revisadas por el departamento de informática, para dictar una directiva sujetándose al estado de derecho.