POLÍTICA DE SEGURIDAD INFORMÁTICA
EVO-GUIA-HSQ-016
Diciembre de 2021. Versión 2

La presente política de Seguridad Informática de Evolucionar Servicios de Salud SAS, establece reglas, normas, controles y procedimientos con el fin de prevenir, proteger y mantener los riesgos de seguridad informática de acuerdo con la Ley Ley estatutaria 1581 de 2012 y demás normas concordantes.

La presente política podrá ser actualizada en cualquier momento, por lo cual se recomienda revisarla con regularidad para asegurarse de que ha leído la versión más actualizada.

NOTIFICACIONES DE VIOLACIONES DE SEGURIDAD

Todo el personal sin importar su tipo de contratación deberá notificar inmediatamente cualquier problema o violación de la seguridad informática que se le presente o del cual sea testigo; esta notificación se puede realizar por medio oral, escrito (carta, correo electrónico) al gerente general, a su jefe inmediato o al coordinador HSQ, quienes estarán obligados de realizar las gestiones pertinentes al caso de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.

De igual manera los trabajadores de Evolucionar Servicios de Salud S.A.S. que maneje datos o información a través de accesos debidamente autorizados, tienen la responsabilidad del cumplimiento de las políticas de control de acceso, de lo contrario podrán incurrir en sanciones administrativas y legales. Por lo que estos trabajadores deberán conocer y respetar las políticas de seguridad. Al igual la empresa debe comunicarle estas responsabilidades, sanciones y medidas en a los trabajadores.

ADQUISICIÓN DE BIENES INFORMÁTICOS

Solamente los responsables de realizar las solicitudes de compras según el procedimiento EVO-PROC-HSQ-011 Procedimiento de compras o servicios aprobará las compras de tecnología informática, todo este proceso después de haber establecido y planeado las prioridades de adquisición. La selección y evaluación de proveedores se realizará de acuerdo con el procedimiento EVO-PROC-HSQ-018 Procedimiento de selección y evaluación de proveedores.

CAPACIDADES

Si la demanda actual se satisface de acuerdo con la carga de trabajo no será necesaria la adquisición de nuevos hardware. Sin embargo, cuando se requiera adquirir hardware se contemplará lo siguiente:

- Los equipos deberán contar con una garantía mínima de un año y deberá contar con el servicio técnico en la ciudad.
- Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de trasferencia de datos, como en procesamiento.
- Las impresoras deberán apegarse a los estándares de hardware y software vigentes en el mercado y la organización, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Juntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
- Se realizará mantenimiento preventivo a los equipos de cómputo, servidores y otros equipos. Este mantenimiento tendrá su seguimiento en la matriz de mantenimiento y calibración de Evolucionar.
- En la adquisición de equipos de cómputo se deberá incluir el software vigente precargado con su licencia correspondiente.

SOFTWARE.

El software autorizado por la compañía estará relacionado en la siguiente lista.

- Sistemas operativos autorizados:
  - Windows 10 bajo licencia.
  - Linux Server software libre
- Ofimática.
  - Office 365 bajo licencia.
- Comprimir.
  - 7 zip software libre.
- Lector PDF.
  - Adobe Reader.
  - EDGE Microsoft.
- Navegadores WEB.
  - Google Chrome.
  - EDGE Microsoft.
  - FIREFOX.
- Antivirus.

- Forticlient

LICENCIAMIENTO

Los productos de software que se utilicen deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

POLÍTICAS DE SEGURIDAD LÓGICA

Red

- El personal no tiene permitido ver, copiar, alterar o destruir la información que reside en los equipos de cómputo sin el consentimiento explícito del responsable del equipo.
- No se permite el uso de los servicios de la red cuando no cumplan con las labores propiedad de la organización.
- Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la organización y se usarán exclusivamente para actividades relacionas con la labor asignada.
- Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

Servidores

- La información estará centralizada en un servidor FILE SERVER (servidor de archivo) y será consultada en red.
- Se creará un árbol o un bloque de carpetas las cuales serán compartidas bajo esquemas de seguridad.
- Las carpetas se crearán bajo los nombres de áreas o departamentos, las cuales se otorgarán permisos de ingresos de acuerdo con el perfil.
- Los usuarios deben estar en grupos de acuerdo con su rol en la compañía, de esta manera se otorgarán los permisos.
- Permisos de ingreso carpetas; los permisos solo son autorizados solo por solicitud de personal autorizados de acuerdo con el organigrama entregado al profesional de tecnología.
- Las solitudes de ingreso deben ser reportadas por e-mail con copia a gerencia o departamento de RH.
- No se deben guardar documentos de manera local, ya que se deben trabajar en RED por temas de administración.

BACKUP.

- Se realizarán copias de seguridad bajo calendario de acuerdo con la prioridad de la información.
- Las copias se identificarán de manera incremental y diferencial.
- Se realizan las copias de 2 manera:

A- Una unidad externa (disco, NAS o SAN)
B- Se tendrá un espacio en la NUBE.

Acceso de usuario al equipo

- Se cuentan con 2 perfiles de ACCESO el de usuario con privilegios limitados y un perfil administrador, con el objetivo de evitar instalaciones de software que no estén de acorde con las políticas de la compañía.
- Cada usuario debe ingresar con una contraseña la cual será responsabilidad de él.

Navegación WEB.

- Esta actividad ayudara a identificar los puntos de inseguridad para evitar ataques y perdida de datos.
- La navegación web será monitoreada con el objetivo de evitar fuga de información e ingresos a sitios que puedan afectar la operación de la compañía.
- Ayuda a identificar los sitios web que más consumen ancho de banda lo cual ayudara a mejorar la calidad de navegación a la internet.

Correo electrónico

- La persona designada se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
- La cuenta será activada en el momento en el que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

Base de datos

- El administrador de la base de datos no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.
- El administrador de la base de datos es el encargado de asignar las cuentas a los usuarios para el uso.
- Las contraseñas serán asignadas por el administrador de la base de datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable del equipo.
- En caso de olvido de contraseña de un usuario, será necesario que se presente con el administrador de la base de datos para reasignarle su contraseña.

Usuarios

- Todos los usuarios con acceso a un sistema de información o a la red, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.

- Los usuarios recibirán un identificador de acceso a la red, recursos informáticos o aplicaciones hasta que no acepte formalmente la política de seguridad vigente.
- El usuario deberá definir su contraseña y será responsable de la confidencialidad de esta.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El usuario deberá notificar al Coordinador Administrativo o al Asesor informático en caso de observar cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor, o si tiene problemas en el acceso a los servicios proporcionados por el servidor.
- Si un usuario viola las políticas de uso de los servidores, el asesor informático podrá cancelar toralmente su cuenta de acceso a los servidores, notificando a la gerencia.
- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque disponga de la autorización del propietario.
- En caso de que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- Cuando el usuario entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

USO APROPIADO DE LOS RECURSOS

Los recursos informáticos, datos, software, red y sistemas de comunicación están disponibles exclusivamente para cumplir las obligaciones y propósito de la operatividad para la que fueron diseñadas e implementadas. Todo usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso. De igual forma queda prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación de uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del software.

- Introducir en los sistemas de información o en la red interna de Evolucionar contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño a los recursos informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Estas políticas cuentan con un alto nivel de compromiso Gerencial, Evolucionar cumplirá y comunicará a sus empleados esta política para obtener su participación y colaboración.

DIANAOBANDO POLO
Gerente General