POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

DELTAS SIS S.A.S.

EN CUMPLIMIENTO A LA

LEY 1581 DE 2012

Ley 1712 DE 2014

DECRETO 1377 DE 2013

CONPES 3701 de 2011

CONPES 3854 de 2016

Y

POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN DE DELTA SIS S.A.S

27 DE MARZO DE 2024

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE DELTA SIS S.A.S.

En DELTA SIS S.A.S la información es un activo fundamental para la prestación de sus servicios, la preservación de los procesos de aseguramiento de seguridad y calidad, y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus datos más significativos 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 sus necesidades actuales, DELTA SIS S.A.S 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, de negocio vigentes y complementa la política de tratamiento de la información de la empresa (Ley 1581 de 2012 y decreto 1377 de 2013).

El proceso de análisis de riesgos de los activos de información que se hizo en DELTA SIS S.A.S, es el soporte del sistema de gestión de la seguridad para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados, tendiente a obtener los niveles de protección de la información esperados en DELTA SIS S.A.S; este proceso será liderado de manera permanente por el director del sistema de gestión de la seguridad y calidad y apoyado de manera irrestricta, por la gerencia.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos, la valoración de análisis de riesgos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados en la identificación de riesgos.

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

DELTA SIS S.A.S ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

1. La gerencia y el director del sistema de gestión de la seguridad y la calidad y quien estos convoquen serán los responsables del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información de DELTA SIS S.A.S.

2. Los activos de información de DELTA SIS S.A.S, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

3. DELTA SIS S.A.S definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Empresa.

4. Todos los empleados y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción no autorizada o uso indebido.

5. Se realizarán auditorías y controles eventuales sobre el modelo de gestión de Seguridad de la Información de DELTA SIS S.A.S.

6. Es responsabilidad de todos los funcionarios y contratistas de DELTA SIS S.A.S reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifiquen.

7. Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

8. DELTA SIS S.A.S contará con un Plan de Continuidad del Negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales que sean catastróficos y/o que amenacen la continuidad en las operaciones de la empresa.

Adicionalmente DELTA SIS S.A.S cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

ACUERDOS DE CONFIDENCIALIDAD

Todos los funcionarios de DELTA SIS S.A.S y/o terceros que manejen información de la empresa deben aceptar los acuerdos de confidencialidad definidos por la empresa, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de los prestadores de servicios, también deberán firmar los respectivos acuerdos de confidencialidad.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de DELTA SIS S.A.S a personas o entidades externas.

Estos acuerdos deben aceptarse por todos los involucrados en los procesos de manejo de información como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

RIESGOS RELACIONADOS CON TERCEROS

DELTA SIS S.A.S identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros y/o contratantes, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establezcan como necesarios a partir del análisis de riesgos que desarrolló DELTA SIS S.A.S, deben ser comunicados y aceptados por el tercero, preferiblemente mediante la firma de acuerdos o a través de cualquier otro medio documental (Puede ser email), previamente a la entrega de los accesos requeridos.

USO ADECUADO DE LOS ACTIVOS

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos de la empresa, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinados por la gerencia o el director del sistema de gestión de la seguridad y calidad.

Para la consulta de documentos cargados del sistema de gestión de la seguridad y la calidad se establecerán privilegios de acceso a los funcionarios y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Director del sistema de gestión de la seguridad y la calidad y se comunicará a la gerencia. Se elaborará un listado con los funcionarios y sus

privilegios. Este listado deberá actualizarse cada vez que un funcionario cambie de cargo o se retire de la empresa.

Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un “acuerdo de confidencialidad de la información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información y la política de tratamiento de datos personales; y que cualquier violación a lo establecido en este parágrafo será considerado como un “incidente de seguridad” y podrá dar lugar a la cancelación del contrato.

ACCESO A INTERNET

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de DELTA SIS S.A.S, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, YouTube, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de DELTA SIS S.A.S.
- El intercambio no autorizado de información de propiedad de DELTA SIS S.A.S, de sus clientes y/o de sus funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el director del sistema de gestión de la seguridad y la calidad o a quien este delegue de forma explícita para esta función,

asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- Solo las personas autorizadas para la remisión de información vía internet podrán hacerlo, nadie más podrá tomar contacto con los clientes o proveedores, sin la debida autorización.
- Nadie podrá acceder a su email personal utilizando los recursos de la empresa.

b) DELTA SIS S.A.S podrá realizar monitoreo de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros que utilicen los medios de la empresa. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente. Nadie podrá hacer uso de los recursos de la empresa para almacenar información personal o acceder a páginas de tipo personal.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d) Los funcionarios y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de DELTA SIS S.A.S, posiciones personales en encuestas de opinión, foros u otros medios similares.

e) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad, los protocolos o la protección de la información de DELTA SIS S.A.S.

CORREO ELECTRÓNICO

Los funcionarios y terceros autorizados a quienes DELTA SIS S.A.S les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del DELTA SIS S.A.S, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar los protocolos de la empresa, la productividad o la protección de la información de DELTA SIS S.A.S.

b) Los mensajes y la información contenida en los equipos y los buzones de correo, son propiedad del DELTA SIS S.A.S y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones y actividades empresariales.

c) El tamaño de los buzones de correo es determinado por el director del sistema de gestión de la seguridad y la calidad, de acuerdo con las necesidades de cada usuario.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por la dirección del sistema de gestión de la seguridad y la calidad.

e) No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no empresarial o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la empresa, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de DELTA SIS S.A.S como punto de contacto en comunidades interactivas de contacto social, tales como Facebook y/o MySpace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.
- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección del sistema de gestión de la seguridad y la calidad.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que DELTA SIS S.A.S proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del director del sistema de gestión de la seguridad y la calidad. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser

enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular, por ejemplo: comercial@deltasis.com.co.

h) Toda información de DELTA SIS S.A.S generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, por ejemplo PDF. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

i) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por DELTA SIS S.A.S y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad cuando se requiera. También deberá conservar el encabezado establecido por la empresa y la leyenda de “Copia no controlada”.

RECURSOS TECNOLÓGICOS

El uso adecuado de los recursos tecnológicos asignados por DELTA SIS S.A.S a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de DELTA SIS S.A.S es responsabilidad de la dirección del sistema de gestión de la seguridad y calidad, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por DELTA SIS S.A.S a través de esta Dirección.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por la Dirección del sistema de gestión de la seguridad y la calidad.

c) La dirección del sistema de gestión de la seguridad y calidad debe definir y actualizar, cuando lo considere oportuno o cuando sea requerido, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios.

d) Únicamente los funcionarios y terceros autorizados por La dirección del sistema de gestión de la seguridad y calidad, previa solicitud por parte de quien lo requiera, pueden conectarse a la red inalámbrica de DELTA SIS S.A.S.

e) La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de DELTA SIS S.A.S, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por La dirección del sistema de gestión de la seguridad y calidad.

f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de DELTA SIS S.A.S; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por La dirección del sistema de gestión de la seguridad y calidad.

g) La sincronización de dispositivos móviles, tales como PDAs, Smartphone, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Empresa, debe estar autorizado de forma explícita por la dirección del sistema de gestión de la seguridad y calidad y podrá llevarse a cabo sólo en dispositivos provistos por la Empresa, para tal fin.

CONTROL DE ACCESO FÍSICO

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico y de advertencia, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales. Deberán adoptarse medidas para tratar de proteger los equipos e información de incidentes tales como; robo, incendios e inundaciones.

PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS

Los equipos que hacen parte de la infraestructura tecnológica de DELTA SIS S.A.S tales como estaciones de trabajo y dispositivos de almacenamiento y/o

comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros. Los equipos que tengan que salir de las instalaciones de la empresa deberán ser entregados con el respectivo recibo y solo a personas que hayan firmado acuerdo de confidencialidad.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de DELTA SIS S.A.S no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos y mucho menos en las salas de poligrafía excepto que se requiera para lo continuación del proceso.

SEGREGACIÓN DE FUNCIONES

Toda tarea en la cual los funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización. En cuanto al acceso al software de poligrafía cada empleado o contratista tendrá un nombre de usuario y contraseña individual para su acceso.

En concordancia:

- Todos los sistemas de disponibilidad crítica o media de la empresa, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza. Se establecerán en el software poligráfico niveles de administración.
- El nivel administrador del software poligráfico recaerá sobre la gerencia y la dirección del sistema de seguridad y de la información, de tal forma que exista una supervisión a las actividades realizadas en el sistema poligráfico.

DELTA SIS S.A.S establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam,

antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, incluyendo claves. Será responsabilidad de La dirección del sistema de gestión de la seguridad y calidad autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización.

Así mismo, DELTA SIS S.A.S define los siguientes lineamientos:

a) No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por DELTA SIS S.A.S.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

COPIAS DE RESPALDO

DELTA SIS S.A.S debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por La dirección del sistema de gestión de la seguridad y calidad y la gerencia, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

La dirección del sistema de gestión de la seguridad y calidad establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con la gerencia los períodos de retención de la misma, de tal forma que sea concordante con la política de tratamiento de la información personal.

Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser respaldados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta la copia original. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados y cumplir con máximas medidas de protección y seguridad física apropiados.

GESTIÓN DE MEDIOS REMOVIBLES

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, IPod, celulares, cintas) sobre la infraestructura para el procesamiento de la información de DELTA SIS S.A.S, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

La dirección del sistema de gestión de la seguridad y calidad es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de DELTA SIS S.A.S sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles.

Se elevaran circulares a los empleados y contratistas respecto a las disposiciones generales para el uso de medios móviles y equipos personales de cómputo.

Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de DELTA SIS S.A.S que éste contiene.

INTERCAMBIO DE INFORMACIÓN

DELTA SIS S.A.S establecerá acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución o que tengan que ver con la política de tratamiento de información personal. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán aceptar o comunicar antes de permitir el acceso o uso de dicha información.

Todo funcionario de DELTA SIS S.A.S es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos y en todo caso, nunca podrán ir en contravía de la política de tratamiento de datos personales.

CONTROL DE ACCESO LÓGICO

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de DELTA SIS S.A.S debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por la gerencia, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información y en la política de tratamiento de datos personales.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios y terceros e implementada por la Dirección del sistema de gestión de seguridad y calidad.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de DELTA SIS S.A.S, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

GESTIÓN DE CONTRASEÑAS DE USUARIO

Todos los recursos de información críticos del DELTA SIS S.A.S tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados La dirección del sistema de gestión de la seguridad y calidad.

Todo funcionario o tercero que requiera tener acceso a los sistemas de información del DELTA SIS S.A.S debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password)

asignado por la organización. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas.

ESCRITORIO Y PANTALLA LIMPIA

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de DELTA SIS S.A.S deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general.

Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de acceder a los software´s especializados de la empresa utilizando un usuario y contraseña y esta nunca deberá ser prestada a un tercero. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz (fondo de pantalla) y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (10) minutos de inactividad. Los equipos de poligrafía no requerirán contraseña de acceso al equipo, sin embargo si se tendrá un usuario y contraseña personalizado para ingresar al software poligráfico.

IDENTIFICACIÓN DE REQUERIMIENTOS DE SEGURIDAD

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en DELTA SIS S.A.S, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad de La dirección del sistema de gestión de la seguridad y calidad y la gerencia.

POLÍTICA DE BACK UP

La presente política general de seguridad de la información va alineada con nuestro sistema de gestión de la seguridad y la calidad, con nuestra política de tratamiento

de la información y con nuestros protocolos poligráficos y de visitas domiciliarias, por lo tanto, a partir de la fecha se dispone que:

- Se debe hacer back up semanal de todos los archivos poligráficos (AP) de la empresa, el cual deberá reposar en la caja fuerte de la empresa.
- Se debe hacer copia de respaldo del Back Up de archivos poligráficos al menos una vez al mes. Esta copia de respaldo deberá reposar fuera de la empresa y en un sitio que garantice las mismas características de seguridad física, del back up que reposa en la caja fuerte de la empresa.
- Se deberá crear una carpeta que contenga todo el soporte de cada proceso de confiabilidad por cada una de los clientes y se hará back up de estas carpetas al menos una vez al mes.

ENTREGA DE INFORMES

Debido a que la información contenida en los informes de los diferentes procesos (Confiabilidad y Poligrafías), son de carácter confidencial y algunos hacen parte de la política de tratamiento de datos personales, DELTA SIS S.A.S, dispone las siguientes orientaciones respecto a la entrega de informes.

- No se deberá imprimir ningún informe de ningún proceso, excepto que el contrato con el cliente así lo disponga.
- Todos los informes que se remitan se harán vía email y en formato PDF, para evitar su adulteración o modificación.
- Se deberá firmar acuerdo de confidencialidad con los clientes en el cual se aclare que la custodia de la información contenida en los diferentes informes corresponden al cliente una vez llegue a su poder.
- Los informes que reposen en la empresa, deberán hacerlo en formato digital y adherirsen a la política de Back Up.
- En caso que algún cliente requiera que se le entreguen informes impresos, estos se deberán entregar con la respectiva constancia de recibo. En la empresa no reposarán copias impresas de dichos informes.
- Los informes de los diferentes procesos que se almacén de manera digital deberán tener una organización e indexación adecuada para facilitar su consulta.
- Se deberá acordar con los clientes que cuando se haga transferencia de datos, estos se destruirán de nuestras bases de datos, de tal forma que si llegare a haber filtraciones de información, estas no se pudieran endilgar a DELTA.

SEGURIDAD DE LA INFORMACIÓN CON LOS VISITANTES

Se asimila al Procedimiento de Manejo de Visitantes. Extracto: En ningún momento los visitantes deberán deambular solos por las instalaciones y deberán ser acompañados hasta su salida de las mismas. Todo visitante debe identificarse en la recepción y ninguna persona foránea deberá tener acceso a los equipos de cómputo, excepto expresa autorización del director del sistema de gestión de la seguridad y calidad.

No deben quedar documentos de la empresa al alcance de personas no autorizadas, excepto aquellas copias no controladas que se requieran para la gestión de los procesos o que son de tipo informativo.

Cada jefe de área, será el primer responsable del resguardo de la información física y digital de que disponga, y del control de las personas que visiten su área.

Los equipos e información siempre deberán estar fuera del alcance de visitantes.

RESUMEN DEL PROCEDIMIENTO PARA EL CONTROL DE VISITANTES

ETAPA		DESCRIPCIÓN	RESPONSABLE
1	**Recepción de Visitante o Empleado**	Se recibe al visitante, se le pide que se registre en el libro de control de visitantes y se contrasta la identidad del visitante con su respectivo documento de identificación, paralela mente se le solicita al área y persona a visitar que confirme la visita, si es evaluado se contrasta con la planilla diaria de evaluaciones. En caso de ser funcionario de la Organización no se le pedirá que se identifique.	Secretaria de Recepción
2	**Autorización de ingreso**	La recepcionista autoriza el ingreso de las personas a las instalaciones y delega la responsabilidad de la custodia del visitantes a la dependencia que corresponda.	Secretaria de Recepción

ETAPA		DESCRIPCIÓN	RESPONSABLE
3	**Recepción de Visita**	Principal: El funcionario debe recibir al visitante en la recepción y acompañarlo al área correspondiente. El visitante en ningún momento deberá permanecer solo dentro de las instalaciones. Al salir deberá ser acompañado hasta la salida y anunciado su retiro en la recepción dejando el registro de hora de salida en el respectivo libro. Este procedimiento se aplicará, tanto para visitantes del área administrativa, como para evaluados de poligrafía u otros procesos de confiabilidad.	Funcionario y Secretaria Recepcionista
4	**Verificación de procedimiento**	En la cartelera y la web permanecerán expuestas las recomendaciones generales, de protección ambiental y de seguridad industrial para visitantes.	Dirección de Calidad.
5	**Información y equipos de computo**	No deberá quedar información sensible o equipos de cómputo expuestos en lugares donde puedan ser manipulados o accedidos por visitantes o evaluados. Las memorias USB, estarán bajo custodia y control de la dirección administrativa. Se les debe advertir a los visitantes que no puede tocar ningún equipo de cómputo o documento sin autorización. Nadie podrá ingresar memorias USB o equipos de computo a las instalaciones, sin la autorización de la dirección administrativa.	Jefe de cada área y recepcionista
6	**Autorización especial**	Las personas que requieran ingresar para la prestación de un servicio eventual o para actividades de mantenimiento deberán ser autorizadas por la gerencia o la persona de más alta jerarquía que se encuentre en las instalaciones, previa coordinación.	Gerencia

ETAPA		DESCRIPCIÓN	RESPONSABLE
7	**Persona no autorizada para ingreso**	Tan pronto es anunciado el visitante y el responsable de recibirlo aclara que por una u otra causa es persona no autorizada para ingreso, inmediatamente se le solicitará el retiro de las instalaciones y se acompañará hasta la salida.	Jefe de cada área.
8	**Ingreso de elementos prohibidos**	La empresa ha generado una política que prohíbe el ingreso a las instalaciones de ciertos elementos, por ello se debe advertir y preguntar al visitante respecto a estos elementos: Se prohíbe el ingreso de armas de fuego, computadores, USB o cámaras a las instalaciones, así como cualquier sustancia química que pudiera generar afectación sobre la integridad de las personas o extracción de información. Está prohibido el uso de celulares dentro de las instalaciones, por lo que se le debe solicitar al visitante que proceda a apagarlos.	Recepcionista y jefe de área
9	**Obligatoriedad de acompañante**	Está prohibido desplazarse sin acompañante por las instalaciones de la empresa y mucho menos desplazarse a lugares a los cuales el visitante no ha sido autorizado, de lo contrario se le pedirá el retiro de las mismas.	Jefe de área
10	**Alcohol y drogas**	No se permite el ingreso de personas en estado de alicoramiento o bajo efectos de drogas alucinógenas. Por ello se deberá indagar al respecto. Está absolutamente prohibido fumar o ingerir licor dentro de las instalaciones. Por lo tanto, se les debe advertir a los visitantes.	Recepcionista y jefe de área.