POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H.

Acuerdos de confidencialidad
[ISO/IEC 27001:2005 A.6.1.5]

Todos los colaboradores del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la organización, 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 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 del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. a personas o entidades externas.
Estos acuerdos deben aceptarse por cada uno de ellos 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
[ISO/IEC 27001:2005 A.6.2.2]

El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. 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, 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, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

Uso adecuado de los activos

[ISO/IEC 27001:2005 A.7.1.3] [Acuerdos 047 y 056 de 2000 Archivo General de la Nación]

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los colaboradores y contratistas determinadas por los directores o coordinadores de área.

Todos los colaboradores 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 que cualquier violación a lo establecido en este parágrafo será considerado como un "incidente de seguridad".

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 del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., 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, Twitter, Whatsapp, Kazaa, MSN Messenger, Youtube, Dropbox, 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 del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H.

- ✓ El intercambio no autorizado de información de propiedad del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., de sus clientes y/o de sus colaboradores, 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 Jefe respectivo y la Coordinación de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los colaboradores y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

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 colaboradores y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., 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 ni la protección de la información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H.
El colaborador cuyo cargo tenga la función de community manager de la organización, deberá hacer el uso adecuado de las redes sociales, garantizando el buen nombre de la organización y la confidencialidad de la información a la que tenga acceso.

Correo electrónico

Los colaboradores y terceros autorizados a quienes el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. 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 CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., no debe ser usada para uso personal y en caso de que por alguna razón tuviera que hacerlo debe realizarse de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por la Coordinación de Tecnología de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por la Coordinación de Tecnología.

e) No es permitido:

- ✓ Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo 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 organización, 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 del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. como punto de contacto en comunidades interactivas de contacto social, tales como *Facebook, twitter, youtube, Instagram, myspace,* entre otras, o cualquier otro sitio que no tenga relación con las actividades laborales.

- ✓ El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- ✓ El envío de correos que superen los 10 MB de tamaño de archivos adjuntos.

- ✓ 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 respectiva y la Coordinación de Tecnología.

- ✓ La configuración del correo electrónico en celulares, ipad, portátiles y equipos tecnológicos en general que no sean de propiedad del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H.. Ver numeral G de recursos tecnológicos.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) El envío masivo de mensajes publicitarios desde cuentas corporativas deberá coordinarse con SIMEC mediante la plataforma designada para ello para que cumpla con los requerimientos de ley

donde se incluya un mensaje que le indique al destinatario como ser eliminado de la lista de distribución, se debe enviar sólo a los correos que nos hayan autorizado para tal fin o a los que por contrato legal tengamos que enviar una comunicación. se debe garantizar el cumplimiento de la Ley de Protección de Datos Personales 1581 de 2013.

h) Toda información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. generada con los diferentes programas computacionales, 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, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Coordinación de Tecnología. 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. Se debe garantizar en todo momento el cumplimiento de la Ley de Protección de Datos Personales.

i) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. a sus colaboradores y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., es responsabilidad de la Coordinación de Tecnología, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. a través de esta Coordinación.

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 Coordinación de Tecnología.

c) La Coordinación de Tecnología debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Únicamente los colaboradores que por sus funciones sean autorizados por la gerencia o porque lo hayan solicitado al área de tecnología y haya sido aprobado en cumplimiento de sus funciones y en las condiciones recomendadas en el momento de la aprobación y los visitantes autorizados por un funcionario como invitado, pueden conectarse a la red inalámbrica del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., acogiéndose a las mismas políticas que aplican para los colaboradores del centro comercial.

e) No está permitido el uso de equipos tecnológicos personales en las redes corporativas del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H..

f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H.; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Coordinación de Tecnología.

g) La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la organización, debe estar autorizado de forma explícita por la dependencia respectiva,

en conjunto con la Coordinación de Tecnología y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.

h) Los dispositivos móviles como computadores portátiles y tabletas de propiedad del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., asignados a colaboradores que requieran por el ejercicio de sus funciones cambiar la ubicación de los mismos, deberán ser controlados, para garantizar la confidencialidad de la información y las conexiones realizadas desde los mismos hacia internet, deberá realizarse a través de conexiones privadas.

Seguridad de Recursos Humanos

[ISO/IEC 27001:2005 A.8 A.8.1 Antes de la contratación Laboral]

El personal contratado para labores donde se tenga acceso a información sensible o confidencial, deberá ser analizado bajo los parámetros específicos de seguridad definidos para el perfil, firmar los acuerdos de confidencialidad a los que haya lugar, y en sus contratos de trabajo deberá hacerse referencia expresa a sus responsabilidades en materia de seguridad.

[ISO/IEC 27001:2005 A.8 A.8.2 Durante la contratación Laboral]

Los accesos a la información se asignarán con base al cargo a desempeñar y sólo para sus funciones específicas.

Se le dotará de los activos necesarios para su actividad, y su uso deberá realizarse con base en las políticas de seguridad definidas.

Deberá realizarse una capacitación continuada en temas de seguridad de la información, con especial atención a aquellas personas que tengan acceso a datos de información de carácter personal contemplado en la ley.

[ISO/IEC 27001:2005 A.8 A.8.3 Terminación o cambio de contratación laboral]

El retiro del personal deberá realizarse de una manera ordenada, con el fin de corroborar todas las acciones requeridas para garantizar que la información se regirá bajo los acuerdos de confidencialidad y responsabilidades definidas en el contrato laboral, con el fin que evitar los riesgos

de robo, pérdida o corrupción de la información. Esto aplica a colaboradores, contratistas o terceras personas.

Es función del responsable de Desarrollo Humano realizar el proceso de terminación general de contratación laboral y debe trabajar junto con el jefe a cargo de la persona, para manejar los aspectos de seguridad de los procedimientos relevantes.

Se debe informar a los usuarios colaboradores, contratistas o terceras personas, de los cambios de personal y los acuerdos de operación.

Todos los usuarios colaboradores, contratistas y terceras personas, deben devolver los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato o acuerdo.

Se deben devolver dispositivos de cómputo móviles, teléfonos, tarjetas de crédito, tarjetas de acceso, software, manuales e información almacenada en medios electrónicos.

En casos donde el usuario colaborador, contratista o tercera persona compra el equipo de la organización o utiliza su propio equipo, se debe garantizar la transferencia y eliminación de la información de la organización del equipo, antes del retiro del funcionario.

En los casos donde el usuario colaborador, contratista o tercera persona tiene conocimiento que es importante para las operaciones actuales, esa información deberá ser debidamente documentada y transferida a la organización.

Los derechos de acceso en caso de terminación deberán ser eliminados en el momento que se considere justo para proteger la confidencialidad e integridad de la información. Si se trata de un cambio de cargo, se deben hacer los ajustes para el nuevo cargo, limitando lo que no corresponda con las nuevas funciones para garantizar la segregación de funciones. Esta restricción incluye acceso físico y lógico, llaves, tarjetas de identificación, medios de procesamiento de información,

suscripciones y retiro de cualquier documentación que identifique a la persona como miembro actual de la organización.

Si el usuario que se retira conoce las claves secretas para las cuentas aún activas, éstas se deben cambiar a la terminación del contrato o acuerdo.
Los derechos de acceso para los activos de información y los medios de procesamiento de información se deben retirar o reducir antes de la terminación, dependiendo de la evaluación de los factures de riesgo como:

a) si la terminación o cambio es iniciado por el usuario colaborador, contratista o tercera persona, o por la gerencia y la razón de la terminación;
b) las responsabilidades actuales del usuario colaborador, contratista o cualquier otro usuario;
c) el valor de los activos actualmente disponibles.

En casos de terminaciones iniciadas por la gerencia, los colaboradores, contratistas o terceros descontentos pueden corromper la información deliberadamente o sabotear los medios de procesamiento de la información. En caso de las personas que renuncian, pueden tratar de recolectar información para su uso futuro.

Control de acceso físico
[ISO/IEC 27001:2005 A.9.1]

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 en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Protección y ubicación de los equipos

[ISO/IEC 27001:2005 A.9.2]

Los equipos que hacen parte de la infraestructura tecnológica del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así 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 funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

Segregación de funciones

[ISO/IEC 27001:2005 A.10.1.3]

Toda tarea en la cual los colaboradores 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 concordancia:

Todos los sistemas de disponibilidad crítica o media de la organización, 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.

Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.

El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Deben estar claramente segregadas las funciones de soporte técnico, planificadores y operadores.

Protección contra software malicioso
[ISO/IEC 27001:2005 A.10.4]

El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. establece, que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, anti spam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red corporativa, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la Coordinación de Tecnología 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 permanente.

Así mismo, el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. define los siguientes lineamientos:

a) No está permitido:

- ✓ La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H..
- ✓ 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

[ISO/IEC 27001:2005 A.10.5]

El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Coordinación de Tecnología y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la organización, 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 Coordinación de Tecnología establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. 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 almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Gestión de medios removibles
[ISO/IEC 27001:2005 A.10.7]

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., estará autorizado para aquellos colaboradores cuyo perfil del cargo y funciones lo requiera.
La Coordinación de Tecnología es responsable de implementar los controles necesarios para asegurar que en los sistemas de información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. sólo los colaboradores autorizados pueden hacer uso de los medios de almacenamiento removibles. Así mismo, el colaborador se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. que éste contiene.

Intercambio de información
[ISO/IEC 27001:2005 A.10.8]

El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. firmará acuerdos de confidencialidad con los colaboradores, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la organización. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo colaborador del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. 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.

Control de acceso lógico

[ISO/IEC 27001:2005 A.11.1]

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Organización, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por la Coordinación de Tecnología del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H..

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 Coordinación de Tecnología.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., 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
[ISO/IEC 27001:2005 A.11.2.3] 9

Todos los recursos de información críticos del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. deben tener asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada colaborador requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por la Coordinación de Tecnología.
Todo colaborador o tercero que requiera tener acceso a los sistemas de información del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. 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 colaborador debe ser responsable por el buen uso de las credenciales de acceso asignadas, y garantizar que utiliza contraseñas con base a las condiciones de seguridad establecidas en forma y contenido, no usar contraseñas de fácil adivinación.

Escritorio y pantalla limpia
[ISO/IEC 27001:2005 A.11.2.4]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los colaboradores del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. 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 bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. 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 y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

Segregación de redes

[ISO/IEC 27001:2005 A.11.4.5]

La plataforma tecnológica del CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. que soporta los sistemas de información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones de redes de clientes, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La Coordinación de Tecnología es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Organización.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

Identificación de requerimientos de seguridad

[ISO/IEC 27001:2005 A.12.1.1]

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H., 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 Coordinación de Tecnología y las dependencias propietarias del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre el CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad de la Coordinación de Tecnología garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y establecer estos aspectos con las obligaciones contractuales específicas.

Política de Tratamiento de Datos Personales

[Ley 1581 de 2012, Decreto 1074 de 2013 (Decreto 1377 de 2013)]

El CENTRO COMERCIAL SANTAFÉ MEDELLÍN P.H. Ha definido su política de tratamiento de datos personales conforme a las disposiciones de la Ley 1581 de 2013 y el Decreto 1377 de 2013 y está documentada, implementada y publicada en http://www.centrocomercialsantafe.com/medellin/tratamientodatos, así mismo existen al interior de la organización los procedimientos establecidos para garantizar con el cumplimiento de la misma.

_____

Gerente General

V.01 del 29 de Enero de 2018.
R.02 del 29 de Junio de 2018.