PROTOCOLO
POLÍTICAS DE SEGURIDAD INFORMÁTICA

EMPRESAS PÚBLICAS DE CUNDINAMARCA S.A

Dirección de Gestión Recursos Físicos y TI

Contenido

INTRODUCCIÓN

Las políticas de seguridad de la información adoptadas por Empresas Públicas de Cundinamarca S.A. E.S.P., buscan establecer medidas técnicas y organizacionales para garantizar la seguridad de las tecnologías de información, brindando los lineamientos necesarios a sus usuarios sobre las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y el software de la red, así como la información que es procesada y almacenada en los mismos.

Estas políticas son construidas con base en el análisis de riesgos de la información en cada una de las áreas de la organización y es aplicable a todos los colaboradores, contratistas, consultores y demás personas que cuenten con equipo conectado a la red de la Empresa. Así mismo, aplica a todos los equipos y servicios propios o arrendados que utilicen los recursos tecnológicos o la red empresarial.

Con el fin de brindar herramientas tecnológicas que sirvan de soporte a las actividades que se realizan permanentemente en cumplimiento del quehacer organizacional, la Empresa ha implementado diferentes instrumentos para el manejo de la información, los cuales están a disposición de los grupos de interés internos para el efectivo desarrollo de sus actividades empresariales. El uso y operación de estas herramientas informáticas estará regido por las políticas de seguridad adoptadas a través de este documento.

I. SEGURIDAD LÓGICA

1. Longitud mínima de las claves de acceso.

Política: La longitud de las claves debe ser mínima de seis (6) caracteres y debe controlarse en el momento en que el usuario la construye o la selecciona.

2. Palabras claves difíciles de adivinar

Política: Todas las palabras claves escogidas por el usuario para ingresar a los sistemas deben ser difíciles de identificar.

En general, no se deben utilizar palabras de un diccionario, derivados del usuario-ID, series de caracteres comunes tales como "123456". Así mismo, no se deben emplear detalles personales como nombre del esposo, placas del carro, número del seguro y fecha de cumpleaños a menos que estén acompañadas por caracteres adicionales que no tengan ninguna relación. Las palabras claves escogidas por el usuario tampoco deben formar parte de una palabra. Por ejemplo, no se deben emplear nombres propios, sitios geográficos y jerga común.

3. Cambios periódico obligatorio de palabras claves

Política: El sistema debe obligar automáticamente a que todos los usuarios cambien sus palabras claves al menos una vez cada seis meses.

4. Cambio obligatorio de palabras clave al acceder por primera vez el sistema

Política: Las palabras claves inicialmente emitidas por un administrador de seguridad deben ser válidas solamente para la primera conexión del usuario, momento en el cual el usuario debe cambiar la palabra clave antes de realizar cualquier otro trabajo.

5. Utilización de palabras claves diferentes cuando se tiene acceso a varios sistemas

Política: Si un usuario tiene acceso a varios sistemas de información, se deben emplear palabras claves diferentes para cada uno de los sistemas a los cuales tiene acceso.

6. No se debe compartir passwords

Política: No importa las circunstancias, los passwords nunca deben ser compartidos o revelados a nadie más que al usuario autorizado. Hacerlo expone al usuario autorizado a responsabilizarse de acciones que otras personas hagan con la palabra clave. Si los usuarios necesitan compartir información permanente del computador, ellos deben usar correo electrónico, directorios públicos, en los servidores de red del área local u otros mecanismos.

7. Cambio de clave cuando se sospecha que ha sido descubierta

Política: Todas las palabras claves se deben cambiar tan pronto como se sospeche que han sido descubiertas o que podrían conocerlas personas no autorizadas.

8. Usuarios responsables de todas las actividades involucrando su código de identificación de usuario

Política: Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario. Los códigos de identificación de usuario no pueden ser utilizados por nadie más, sino por aquellos a quienes se les ha expedido. Los usuarios no deben permitir que otros realicen ninguna actividad con sus códigos de identificación de usuario.

9. Log-Off (fuera del login) de los computadores personales conectados a las redes

Política: Si los computadores personales (PCs) están conectados a una red, cuando no estén en uso se debe salir siempre de todas las aplicaciones a que haya ingresado y no exponer el computador a ingresos NO autorizados.

II. USO DE LOS SISTEMAS

10. Uso personal del computador y sistemas de comunicación

Política: El computador de la Empresa y los sistemas de comunicación deben usarse solamente para asuntos de la empresa.

11. Alteraciones/Expansiones hechas a los Computadores dotados por la Empresa

Política: Los equipos de cómputo de la Empresa no deben ser alterados ni mejorados en ninguna forma (ejemplo: actualización de procesador, expansión de memoria o adición de otras tarjetas) sin el conocimiento y autorización del responsable del departamento.

12. Reporte de los Daños de Hardware – Software pertenecientes a la Empresa

Política: Los colaboradores deben reportar inmediatamente a los administradores de TI sobre cualquier daño o pérdida del equipo, software o información que tengan a su cuidado y sean propiedad de la Empresa.

13. No se deben almacenar juegos en los computadores de la Empresa.

Política: No deben almacenarse ni usarse juegos en ninguno de los sistemas del computador de la Empresa.

14. Permiso para uso personal ocasional de los sistemas de la Empresa

Política: Los sistemas de información de la Empresa deben usarse solamente para trabajos relacionados con las actividades de la misma. El uso personal ocasional puede permitirse si : (a) no se consume más que una cantidad mínima de los recursos que podrían, en otra forma, usarse para asuntos de negocios, (b) no interfiere con la productividad del trabajador, y (c) no se apropia de ningún tipo de actividad comercial.

Si esta exploración es para fines personales, debe hacerse en sus horas libres, y no en horas de trabajo de la Empresa. Así mismo, noticias, grupos de discusión, y otras actividades que definitivamente no están dentro de sus obligaciones laborales, deben hacerse en las horas libres del empleado y no en horas de trabajo.

15. Usos permitidos de información de la Empresa

Política: La información de la Empresa debe usarse solamente con fines laborales expresamente autorizados por la administración.

16. Conceder códigos de identificación de usuarios a extraños

Política: No se puede conceder, o dar cierto tipo de prerrogativas con los códigos de identificación de usuarios a individuos que sean colaboradores retirados, proveedores, o consultores para usar los computadores de la Empresa, o de los sistemas de comunicación.

17. Las prerrogativas de acceso a los sistemas de información se terminan cuando el trabajador se retira de la Empresa

Política: Todas las prerrogativas para el uso de los sistemas de información de la Empresa deben terminar cuando se tenga conocimiento que el trabajador se retira de la Empresa.

18. Cambios en la configuración del software instalado en los equipos de cómputo

Política: No está permitido el cambio en la configuración estándar del software instalado en los equipos de cómputo, tales como:

- Configuraciones de red
- Fondos de pantalla
- Unidades de red
- Configuraciones de dispositivos (impresoras, scanner)

III. ADMINISTRACIÓN DE CONTROL DE ACCESO A LA INFORMACIÓN

19. Controles de acceso a los computadores principales

Política: Toda la información de los computadores principales (servidores) que sea sensible, crítica o valiosa debe tener controles de acceso al sistema para garantizar que no sea inapropiadamente descubierta, modificada, o borrada.

20. Capacidades del usuario para el acceso de archivos y su implicación en cuanto al uso

Política: Los usuarios no deben leer, modificar, borrar, o copiar un archivo que pertenezca a otro usuario, sin obtener primero permiso del propietario del archivo. A menos que el acceso general haya sido claramente proporcionado, la habilidad para leer, modificar, borrar, o copiar un archivo que pertenezca a otro usuario no implica que el usuario tenga permiso para realizar estas actividades.

21. Códigos de identificación de computadores únicos.

Política: Cada computador o sistema de comunicaciones debe tener una única identificación. Códigos de identificación de equipos para grupos o que sean compartidos no son permitidos.

IV. ACTIVIDADES ADMINISTRATIVAS

22. Revisión periódica y reevaluación de los privilegios de acceso del usuario.

Política: La Administración debe reevaluar el otorgamiento de los privilegios de acceso a los sistemas a todos los usuarios como máximo cada seis (6) meses.

23. Entrega de los códigos de identificación de usuarios.

Política: Los usuarios deben firmar un acuerdo con la Empresa sobre la confidencialidad con el manejo de la información y el acatamiento con las normas de seguridad del sistema, antes de entregárseles los códigos de identificación de usuario para ingresar a los sistemas de la Empresa.

24. Reportes sobre cambios de tareas y responsabilidades.

Política: La Dirección de Gestión Humana y Administrativa o los directores de área, deben informar oportunamente al área de Tecnología sobre todos los cambios de tareas y responsabilidades operativas o administrativas de los colaboradores, retiros e ingresos de nuevos colaboradores, a los administradores de los sistemas de información y del sistema de seguridad para que actualicen, controlen y administren los códigos de identificación de usuarios.

V. VIRUS INFORMÁTICO

25. La eliminación de virus informáticos por parte de los usuarios finales requiere ayuda del administrador del sistema

Política: Se prohíbe a los usuarios finales eliminar virus informáticos de los sistemas de la Empresa, cuando éstos están infectados, en razón de que pueden producir más daños en la información o programas o permitir una reinfección sobre éstos, se debe pedir ayuda de asistencia técnica a los administradores de TI.

26. No se debe bajar y cargar Software de Internet en los sistemas corporativos por parte de terceras personas

Política: Los colaboradores de la Empresa no deben permitir que terceras personas puedan bajar y cargar "down-loading" software de Internet, en los sistemas de la Empresa. Esta prohibición es necesaria porque dicho software puede contener virus, lombrices, caballos Troyanos y otro software que puede dañar la información y los programas en producción.

27. Pruebas de virus antes de usar los programas en la Empresa

Política: Para prevenir la infección por virus en los computadores, los colaboradores de la Empresa no deben usar ningún software proporcionado externamente por una persona u organización que no sea un proveedor conocido y confiable. La única excepción a esto, es cuando el software ha sido primero probado y aprobado por los administradores de TI.

28. Los medios magnéticos proporcionados externamente deben ser previamente examinados contra la presencia de virus

Política: Cualquier medio magnético proporcionado externamente (como CD, DVD, memorias USB o discos duros externos), no pueden utilizarse en ningún computador personal (PC) o servidor de la red local (LAN) de la Empresa, a menos que estos medios hayan sido primero examinados contra virus. Es responsabilidad del usuario hacer esta verificación y cualquier soporte requerido debe ser informado a los administradores de TI.

29. Proceso para examinar el Software obtenido a través de internet

Política: Antes de descomprimir el software obtenido a través de internet los usuarios deben cerrar todas las sesiones activas en los servidores y otras conexiones en red, debe evaluarse la presencia de virus informáticos antes de ejecutarse. Si un virus es detectado debe notificarse inmediatamente al área de tecnología quienes deben colocar un mensaje de alerta vía correo electrónico a todos los usuarios de la red para que se abstengan de bajar este software infectado a través de internet.

30. Los archivos magnéticos deben descomprimirse antes de examinar si están contaminados por Virus

Política: Todos los archivos magnéticos (programas, bases de datos, documentos de texto, etc.) deben ser descomprimidos antes de proceder a hacer una evaluación de virus informáticos. A los programas o archivos comprimidos no se les pueden detectar con facilidad la existencia de virus.

31. Copias de respaldo al software original para microcomputadores

Política: Todo el software original de los computadores personales debe copiarse antes de iniciar su uso, y esas copias deben almacenarse en un lugar seguro y confiable. Estas copias master no deben usarse para actividades comerciales ordinarias, sino que deben reservarse para cuando se presenten infecciones de virus, daños en el disco duro y otros problemas que obligue la restauración del software original.

32. Verificación del software antes de distribuirlo a los usuarios

Política: Antes de distribuir cualquier software a los usuarios, los colaboradores de la Empresa deberán primero someterlo a pruebas exhaustivas, incluso a pruebas que identifiquen la presencia de virus en la computadora.

VI. OPERACIÓN DEL COMPUTADOR

33. No se debe fumar, comer y beber en el Centro de cómputo o cerca de los equipos de computo

Política: Ningún usuario deberá fumar, comer o beber en el Centro de cómputo o en los puestos de trabajo donde se encuentren los equipos tecnológicos. Al hacerlo estarían exponiendo los equipos a daños eléctricos, así como a riesgos de contaminación sobre los dispositivos de almacenamiento de datos. En la mayoría de los casos, los equipos de cómputo comienzan a fallar por cualquiera de las siguientes causas:

- Migajas o sobras de comida en los teclados, impresoras y monitores.
- Líquidos esparcidos sobre el teclado o las impresoras

34. No se debe trasladar los equipos de cómputo sin la autorización y supervisión de los administradores de TI

Política: Ningún usuario puede trasladar, desconectar o conectar equipos de cómputo sin la autorización y supervisión de los administradores de TI. Se busca evitar daños

en los equipos de cómputo por mala manipulación y ejercer un mejor control del inventario de equipos de Cómputo.

35. No se debe modificar la configuración del Software Base o de los equipos de Cómputo

Política: Ningún usuario debe modificar la configuración del Software Base (Sistemas Operativos, Programas antivirus, programas de Mail) como tampoco modificar la configuración de los equipos de cómputo a través del Setup de la máquina. Esto evita problemas de desconfiguración que pueden ocasionar conflictos tanto en el software como en el hardware.

36. Apagar los equipos de cómputo al terminar las labores

Política: Todos los equipos de Cómputo se deben apagar al terminar la jornada laboral o a la hora del almuerzo, con excepción de los Servidores que nunca se deben apagar. Esto evita el uso indebido de los equipos por parte de personas extrañas o ajenas al área, alarga la vida útil de las máquinas, evita el apagado incorrecto y contribuye al ahorro de energía eléctrica.

37. No poner elementos sobre los equipos de Cómputo

Política: No se debe poner ningún elemento sobre los equipos de Cómputo, como por ejemplo Carpetas, materas, adornos, papeles, bolsas, etc. Estos elementos pueden afectar el normal funcionamiento de los equipos por calor excesivo, en el caso que se coloquen elementos que obstruyan los sistemas de ventilación (especialmente sobre los monitores).

38. Todos los equipos de Cómputo se deben conectar al Sistema Regulado de Energía (UPS).

Política: Los equipos de Cómputo deben conectarse a las tomas de corriente Regulada, las cuales se diferencian por el color naranja, o en su defecto por las marquillas "UPS"; excepto las impresoras que deben conectarse a las tomas de corriente **Normal.** En el caso de las impresoras de Inyección de tinta, estas deben conectarse a las tomas de corriente Regulada. Esto evita daños graves en los equipos de Cómputo por problemas eléctricos y garantiza la continuidad de energía y evita la posible pérdida de información en el caso de un corte del fluido eléctrico.

39. No se debe conectar equipos eléctricos diferentes a los Equipos de Cómputo, al Sistema Regulado de energía (UPS).

Política: No se debe conectar ningún equipo eléctrico como por ejemplo taladros, cafeteras, brilladoras, aspiradoras, radios, máquinas de escribir eléctricas, ventiladores o cualquier otro equipo diferente a un equipo de Cómputo, en las tomas de corriente Regulada (las de color naranja); estos equipos solo se pueden conectar en las tomas de corriente **Normal.** Al hacer caso omiso de esta norma puede ocasionar una caída de todo el Sistema Regulado de energía, teniendo como consecuencias la posible pérdida de información o incluso el daño de cualquiera de los equipos de Cómputo conectados a la Red Regulada.

40. Se prohíbe el ingreso de personal NO autorizado a los Centros de cómputo.

Política: Ningún funcionario diferente a los administradores de TI puede ingresar a los Centros de cómputo, esta área debe permanecer con llave y solo se permitirá el ingreso de personas ajenas con la debida autorización y acompañamiento de un funcionario del área de Tecnología.

41. No exponer los equipos de Cómputo a luz solar directa.

Política: No se debe exponer ningún equipo de cómputo a la luz solar directa; colocar persianas o cortinas en las ventanas que no dispongan de esta protección, o cambiar de ubicación los equipos expuestos en el caso de que no sea posible ubicar una protección El calor producido por la luz solar directa puede afectar el funcionamiento de los equipos de Cómputo, y acorta la vida útil del equipo.

42. Cualquier problema o funcionamiento anormal que se presente en la operación de un equipo de Cómputo, debe ser reportado inmediatamente a los administradores de TI.

Política: Los usuarios deben reportar inmediatamente a los administradores de TI cualquier problema técnico que se presente en la operación de un equipo de Cómputo, indicando en la forma más detallada y exacta el tipo de problema presentado.

43. Los usuarios deben apagar correctamente los computadores.

Política: Todos los usuarios deben apagar correctamente los computadores, a través del botón de "inicio", la opción "Apagar el sistema" y luego "Apagar el equipo"; solo cuando aparezca el mensaje "AHORA PUEDE APAGAR EL EQUIPO" se puede apagar con el interruptor de apagado. Los equipos que tienen apagado automático no necesitan apagarse con el interruptor.

44. Todos los trabajos de mantenimiento que involucren el corte de Energía Eléctrica, deben ser coordinados con los administradores de TI

Política: Cualquier trabajo de mantenimiento que se realice en las oficinas de la, y que requiera el corte de energía eléctrica, debe ser informado previamente a los administradores de TI para que se coordine conjuntamente con las personas que realizarán estos trabajos de mantenimiento, y así mismo poder informarles con anticipación a los usuarios.

VII. SEGURIDAD DE LOS DATOS

45. La información se considera el recurso más importante de la Empresa

Política: Es absolutamente esencial que la Empresa proteja la información para garantizar su exactitud, oportunidad y confiabilidad.

La información deberá ser manejada adecuadamente y ser accesible sólo a las personas autorizadas, de acuerdo con el Código de ética y transparencia Empresarial, las normas, políticas y procedimientos Corporativos relacionados con los Sistemas de Información.

46. Todos los derechos de propiedad sobre el software y la documentación desarrollada para uso corporativo son exclusivos de la Empresa.

Política: Sin excepción alguna, todo el Software y su documentación generada y desarrollada por colaboradores, consultores, proveedores o contratistas para el beneficio y uso Corporativo, es propiedad exclusiva de la Empresa.

47. Todos los derechos de propiedad legal sobre archivos fuente de aplicación y mensajes, son exclusivos de la Empresa.

Política: La Empresa tiene propiedad legal sobre el contenido de todos los archivos almacenados en los equipos de cómputo y sistemas en red, así como de todos los mensajes que viajan a través de estos sistemas. La Empresa se reserva el derecho de permitir el acceso a esta información a terceras personas.

48. Reintegro de los recursos suministrados por la Empresa para el desarrollo de trabajos.

Política: Los colaboradores, contratistas y consultores no recibirán sus honorarios o pago final por el trabajo realizado, a menos que hayan devuelto formalmente a la Empresa todo el hardware, software, información y otros materiales que le fueron entregados para la realización de su trabajo.

49. Toda adquisición de software deberá tener su licencia por escrito a nombre de la Empresa

Política: Siempre que la Empresa haya adquirido un software integral, el proveedor deberá proporcionar por escrito la licencia del software.

50. Eliminar el software y la información magnética que no sean de propiedad de la Empresa

Política: El Software y la Información que no son de propiedad de la Empresa, es decir, que no cuente con las respectivas licencias de propiedad intelectual registradas y no tenga autorización específica para su almacenamiento y/o uso, no deberá almacenarse en los equipos, sistemas o redes de la Empresa. Los Administradores del Sistema, eliminarán este software e información.

51. No se debe copiar, transferir o divulgar software.

Política: Los usuarios finales no deberán copiar software proporcionado por la Empresa en ningún medio de almacenamiento magnético o transferir Software de un equipo a otro a través de algún sistema de comunicación, o divulgar software.

52. No se debe usar herramientas para romper la seguridad de los sistemas.

Política: Los colaboradores de la Empresa no deberán adquirir, poseer, comercializar o usar herramientas de hardware o software que pudieran emplearse para evaluar o comprometer la seguridad de los sistemas de información. Si la Empresa considera utilizar este tipo de herramientas tecnológicas para la evaluación de la seguridad de los sistemas, deberán ejecutarse en el ambiente de pruebas.

53. Manejo de la información confidencial de propiedad de terceros.

Política: Toda información confidencial o de propiedad de un tercero, que se ha confiado a la Empresa, deberá ser protegida como si se tratara de información confidencial Corporativa.

54. No se debe transferir información corporativa a terceros sin la autorización expresa de la Gerencia General

Política: El software de la Empresa, su documentación y otros tipos de información interna, no deben ser enviados o trasladados a sitios que no son de la Empresa, sin la autorización de la Gerencia General.

55. El derecho para examinar los datos guardados en los sistemas de la Empresa

Política: La dirección se reserva el derecho de examinar todos los datos guardados o transmitidos en sus sistemas, como las computadoras y los sistemas de comunicaciones de la Empresa.

56. Revelar la información que exija la ley o la que ordene la Dirección General de la Empresa.

Política: Los usuarios deben permitir que toda la información que este en su poder dentro de la Empresa, pueda ser divulgada por instrucciones de ley y a discreción de la Empresa, con el acompañamiento siempre de los administradores de TI.

57. Restricción de revelar información particular de los colaboradores.

Política: La Empresa no revelará los nombres, títulos, números de teléfono, localización u otra información particular de sus colaboradores a menos que sea requerido para propósitos del objeto social de la Empresa. Se harán excepciones cuando dicha revelación sea exigida por ley o cuando las personas involucradas hayan consentido previamente tal revelación de la información.

58. Seguridades para la entrega de información de clientes a terceros

Política: La información recolectada de los clientes, tal como número telefónico y dirección, se debe usar para propósitos internos de la Empresa y se deberá entregar a terceras partes solo si:

- El cliente ha proporcionado su consentimiento anteriormente por escrito,
- Por solicitud escrita de Empresas gubernamentales o entes de control.

VIII. CONFIDENCIALIDAD DE LOS DATOS

59. Confidencialidad de la Información.

Política: Toda la información que tenga carácter confidencial, en los términos establecidos en la ley, deberá enmarcarse en lo establecido en el Código de Ética y Transparencia Empresarial.

60. Aprobación de la Gerencia General para destruir registros de información

Política: Los colaboradores no deben destruir o disponer de la información que es potencialmente importante para la Empresa sin tener una aprobación específica. El individuo que realice intencionalmente una destrucción no autorizada de los registros o información de la Empresa estará sujeto a acciones disciplinarias incluyendo la terminación del contrato y procesos legales. Los registros y la información se deben conservar sí: a) Son necesarios en el futuro, b) las leyes o los estatutos requieren su conservación y, c) en caso de que puedan ser necesitados como pruebas en investigaciones de actos ilícitos, no autorizados o abusos.

61. Manejo de información en desuso e incompleta

Política: Toda información incompleta, obsoleta o en desuso debe ser suprimida y no distribuida al usuario; a menos que este acompañada de una explicación que describa la naturaleza de dicha información como informes preliminares, resultados sujetos a validación, etc.

62. Requisitos para modificar información de valor, sensible o crítica

Política: Toda transacción que afecte información de valor, sensible o crítica debe ser procesada únicamente cuando se valide la autenticidad del origen (usuario o sistema) y se comprueba su autorización mediante un mecanismo de control de acceso o perfiles. Los procesos de autenticación pueden ser realizados a través de contraseñas, tarjetas inteligentes, lectores biométricos, o firmas digitales en correo electrónico o en el sistema de Gestión Documental.

63. Toda información al público debe ser validada con la Dirección de Servicio al Cliente

Política: Toda información al público como home pages, carteleras electrónicas, propaganda en medios escritos y hablados de la Empresa debe ser validada con la Dirección de Servicio al Cliente como responsable de las comunicaciones.

64. Uso de sistemas de comunicación y computadores para emitir opiniones personales de los colaboradores

Política: Los sistemas de comunicación y computadores de la Empresa no deben ser usados para emitir opiniones personales de los colaboradores.

65. Censura de información divulgada por los medios de comunicación de la Empresa

Política: La administración de la Empresa se reserva el derecho de censurar cualquier tipo de información a través de los medios de comunicación y computadores de la Empresa. Las facilidades de comunicación de la Empresa son privadas y no de dominio público.

66. Derecho de la administración de la Empresa a remover material de tipo ofensivo o ilegal

Política: La administración de la Empresa se reserva el derecho a remover de sus sistemas de información, cualquier material que pueda ser ofensivo o ilegal.

67. Persecución étnica, sexual y racial

Política: La persecución étnica, racial o sexual incluyendo llamadas telefónicas anónimas y mensajes de correo anónimos está estrictamente prohibidas y pueden causar sanciones e incluso la terminación del contrato de un colaborador. La administración debe hacer que esta política sea clara a todos los colaboradores e investigar en forma inmediata cualquier ocurrencia sospechosa.

68. Las direcciones internas de la red no deben ser divulgadas públicamente

Política: Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la Empresa deben ser restringidas, de tal forma que no sean conocidas ni por usuarios internos ni clientes o personas ajenas a la organización.

IX. SEGURIDAD EN COMUNICACIONES

69. Mecanismos de control de acceso para computadores conectados a la red

Política: Todos los computadores de la Empresa que puedan ser accedidos por terceros a través de mecanismos como: líneas conmutadas, Internet y otros, deben ser protegidos por mecanismos de control de acceso aprobados por el área de Tecnología.

70. Las conexiones a líneas conmutadas deben pasar siempre a través de un Firewall

Política: Todas las líneas conmutadas que permitan el acceso a la red de comunicaciones o sistemas multi-usuario deben pasar a través de un punto de control adicional (Firewall) antes de que el pantallazo de login aparezca en la terminal del usuario.

71. Conexiones a redes externas de tiempo real deben pasar siempre por un firewall

Política: Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Empresa o sistemas multi - usuario, debe pasar a través de un punto adicional de control como: firewall, servidor de acceso o gateway.

72. La conexión a Internet requiere de implementar un mecanismo de firewall aprobado y certificado

Política: Toda conexión entre los sistemas de comunicación de la Empresa e Internet o cualquier red pública de datos debe incluir un Firewall y otros mecanismos adicionales de control de acceso.

73. Cualquier comunicación externa vía modems o cualquier otro medio de comunicación debe estar aprobada

Política: Los colaboradores y contratistas no deben llevar a cabo ningún tipo de instalación de nuevas líneas telefónicas o canales de transmisión de datos sin haber sido formalmente aprobados por el área de Tecnología.

74. Criterios de conexión de la red interna de la compañía a otros de terceros

Política: La conexión entre sistemas internos de la Empresa y otros de terceros debe ser explícitamente aprobada y certificada por el área de Tecnología el fin de no comprometer la seguridad interna de la información de la Empresa.

75. Requerimientos de seguridad para conectar la red interna de la Empresa a la de terceros

Política: Como requisito para interconectar las redes de la Empresa con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por la Empresa, quien se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La Empresa se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la Empresa.

76. Requisitos de seguridad para trabajar desde la casa o sitio de residencia

Política: El trabajo desde la casa es una decisión del Director del área responsable. Para ello se deben tener en cuenta las siguientes consideraciones: Seguridad física e informática para los recursos de la Empresa, un ambiente de trabajo que no distraiga al empleado, procedimientos para evaluar el rendimiento del empleado y mecanismos apropiados para estar en contacto con otros colaboradores.

77. Divulgación de números de cuentas bancarias

Política: Los números de cuentas bancarias de los clientes son confidenciales y no deben ser divulgadas a terceros.

78. Conexiones remotas a los computadores de la Entidad (por ejemplo con TeamVeawer)

Política: No están permitidas las conexiones remotas a computadores de la entidad a través de herramientas como por ejemplo TeamVeawer. Este tipo de conexiones deben ser previamente autorizadas por el área encargada de Tecnologías de la Información.

X. SISTEMAS TELEFÓNICOS

79. Llamadas Por Cobrar (Gratis para el Usuario) son Prohibidas en Líneas con Correo de Voz (Contestador Automático)

Política: Los administradores a cargo de los sistemas de correo de voz en la Empresa deben hacer arreglos con la compañía de teléfonos para que las llamadas "Por Cobrar" (son llamadas entrantes que paga el receptor y no el originador) sean prohibidas en las líneas telefónicas con correo de voz. Esto evitará que los saqueadores de red y otro personal no autorizado utilicen el sistema de correo de voz a costa de Empresa.

80. Uso de Teléfonos para Uso Personal

Política: Los teléfonos de una Empresa tienen la función de facilitar las actividades comerciales, no deben ser utilizados para propósitos personales, a menos de que estas llamadas no puedan efectuarse fuera de las horas de trabajo. En estos casos las llamadas personales deben ser de una duración razonable y no deben ser de larga distancia.

XI. SISTEMAS DE CORREO ELECTRÓNICO

81. Asignación y responsabilidades sobre el uso del correo Electrónico

Políticas:

- Los colaboradores y contratistas de apoyo de Empresas Públicas de Cundinamarca deben emplear las direcciones de correo electrónico corporativas asignadas para atender los asuntos de la Entidad.
- Todos los colaboradores y contratistas de apoyo a la entidad tienen derecho a tener una cuenta de correo institucional.
- El Director de cada Dependencia debe solicitar al área encargada de las tecnologías de información vía correo electrónico, la creación o bloqueo de una cuenta de correo.
- El área encargada de las Tecnologías de información es la encargada de proporcionar y vigilar el servicio. Para tal fin asignará una cuenta, la cual incluye un buzón de correo donde se almacenan todos los mensajes enviados y recibidos.
- Cada usuario debe depurar continuamente su buzón de correo con el fin de mantener espacio disponible para la recepción de nuevos mensajes.
- Cada usuario es responsable de la información enviada y reenviada desde su cuenta de correo.

82. Restricciones sobre el uso de correos masivos

Políticas:

- No está permitido el envío de correos a "Todas las dependencias" o a un grupo de usuarios, cuyo contenido no sea de carácter institucional. En caso de requerirse envío de información institucional a "Todas las dependencias" o a un grupo de

usuarios, sólo se realiza a través de Servicio al Cliente quien es el responsable de las comunicaciones en la Empresa.

- Al enviar correos a "Todas las dependencias" o a un grupo de usuarios, el tamaño de la información que se incluya en dichos mensajes NO debe ser mayor a 200 Kb.

83. Usando una Cuenta de Correo Electrónico Asignada a Otro Individuo

Política: Los colaboradores no deben utilizar una cuenta de correo electrónico que ha sido asignada a otro individuo ni para enviar ni para recibir información. Si hay necesidad de leer el correo de otra persona (por ejemplo cuando están en vacaciones), remisión de mensajes a otra dirección u otros métodos pueden ser usados preferiblemente.

84. Autorización para Leer Correo Electrónico de Otros Colaboradores

Política: Cuando el Director de Dependencia y el Director de Gestión Humana estén colectivamente de acuerdo, los mensajes de correo electrónico viajando a través de los sistemas de la Empresa pueden ser monitoreados para cumplir con políticas internas, por sospechar la actividad criminal, y otras razones de sistemas de gerencia. A menos de que este trabajo sea específicamente asignado por los gerentes, el monitoreo de los mensajes de correo electrónico está prohibido por cualquier otro trabajador.

85. Restringir el Contenido del mensaje en el Sistema de Información de la Empresa.

Política: Los colaboradores tienen prohibido enviar o remitir por medio del sistema de información de la Empresa, cualquier mensaje que una persona razonable pueda considerar difamatorio, hostil o explícitamente sexual. Los colaboradores también tienen prohibido enviar o remitir mensajes o imágenes por medio del sistema de la Empresa, que puedan ofender las creencias de raza, género, nacionalidad, orientación sexual, religión, creencias políticas o discapacidad.

86. Los Mensajes de Correo Electrónico son Registros de la Empresa.

Política: El sistema de correo electrónico de la Empresa debe ser usado únicamente para propósitos de trabajo. Todos los mensajes enviados por medio del correo electrónico son registros de la Empresa, quien se reserva el derecho de acceder y revelar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Los supervisores deben revisar las comunicaciones de correo electrónico de los colaboradores supervisados para determinar si han atentado contra

la seguridad, violado políticas de la Empresa o ejecutado cualquier otra acción no autorizada. La Empresa también debe revelar los mensajes electrónicos a los oficiales de la ley sin notificación previa a los colaboradores que hayan enviado o recibido este tipo de mensajes.

87. Autorización para hacer Público un Mensaje a través del Correo Electrónico y Correo de Voz.

Política: La herramienta de envío de mensajes masivos a través de correo electrónico y correo de voz pueden ser utilizadas o aprobadas por la alta gerencia o la Dirección de Servicio al Cliente.

XII. PROPIEDAD INTELECTUAL Y SEGURIDAD EN SITIOS DE TRABAJO ALTERNOS

88. Protección de la propiedad de la Empresa en Sitios de Trabajo Alternos

Política: La seguridad de la propiedad de la Empresa, en sitios de trabajo alternos es tan importante como lo es en las oficinas centrales. En sitios de trabajo alterno, se deben tomar precauciones razonables que puedan proteger contra robo, daño y/o mal uso a los equipos, el software y la información.

89. Derechos a Propiedad Intelectual desarrollados en sitios de trabajo alternos

Política: La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Empresa. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, documentación y otros materiales.

90. Ambientes de Trabajo Estructurados y Telecomunicaciones

Política: Para mantener el privilegio de hacer trabajos por fuera, todas las telecomunicaciones deben estructurar su ambiente remoto, para cumplir con las políticas y estándares de la Empresa.

XIII. CONEXIONES DE INTERNET

91. El área encargada de las Tecnologías de Información es la responsable de habilitar o bloquear los accesos a Internet.

Política: Los Administradores de las Tecnologías de la información son los encargados de proporcionar el servicio de acceso a Internet, así como de vigilar su uso correcto y su debido funcionamiento. Igualmente, el área encargada de Tecnologías de la información está autorizada para bloquear aquellos sitios de Internet que considere que no son compatibles con las labores de los colaboradores y contratistas.

92. Restricciones en el uso del internet.

Política: No está permitido el ingreso a páginas de internet que no estén relacionadas con las funciones y responsabilidades de colaboradores o contratistas, tales como:

- Páginas pornográficas así como aquellas que patrocinen personas u organizaciones al margen de la ley o que tengan algún contenido ilegal.
- Descargar programas que faciliten conexiones automáticas.
- Páginas de música o videos en línea
- Descargar música y videos, provistos por páginas especializadas para tal fin.
- Utilizar o participar en juegos de entretenimiento en línea.
- Descargar o instalar programas diferentes a los autorizados por la entidad.
- Modificar los paquetes y configuraciones ya instaladas en los computadores de la Entidad

93. Derechos de Propiedad Intelectual de Otras fuentes en Internet

Política: Aunque el Internet es un ambiente de comunicación informal, aplican las leyes para derechos de reproducción, patentes, marcas registradas, y todo lo relacionado. En este punto, los colaboradores que utilicen sistemas de la Empresa deben por ejemplo: a) publicar material únicamente después de obtener permisos de la fuente, b) indicar fuente únicamente si ésta es identificada y, c) revelar información interna de la Empresa en Internet solo si la información ha sido aprobada oficialmente en un comunicado público.

94. Página Web de la Empresa en Internet

Política: Todos los cambios que se hagan en la página web de la Empresa en Internet deben ser aprobados por la Dirección de Servicio al Cliente antes de ser publicados, con el fin de asegurar que todo el material puesto en la página web contenga una

apariencia consistente y pulida, esté de acuerdo con las metas de la empresa y, protegido por las medidas de seguridad adecuadas.

95. Requerimientos de Diseño de la Página Web en Internet

Política: Todas las páginas web de la Empresa en Internet deben ajustarse a estándares de diseño, navegación, redacción legal, y requerimientos similares establecidos por la Dirección de Servicio al Cliente.

96. Enviar Información de Seguridad y Pagos a través de Internet

Política: Los colaboradores no deben enviar números de tarjetas de crédito, clave de entrada o cualquier otra información de seguridad o pagos por medio del correo electrónico de Internet si esta está en forma legible (no encriptada).

97. La Empresa Bloquea el Acceso a Ciertas Páginas en Internet que no tienen que ver con Negocios

Política: Los sistemas de información de la Empresa rutinariamente previenen a los usuarios de conectarse a determinadas páginas de Internet no relacionados con las actividades de la misma. Los colaboradores que encuentren que se pueden conectar a páginas de Internet que tengan contenidos sexuales, racistas o cualquier otro tipo de material ofensivo deben desconectarse inmediatamente de ese sitio. La posibilidad de conectarse a una página específica por sí mismo no implica que el usuario del sistema de la Empresa tenga el permiso para visitar dichos sitios.

98. Manejo de Software y Archivos bajados de Internet

Política: Todo el software y archivos bajados desde fuentes diferentes a la Empresa a través de Internet (o cualquier otra red pública) deben ser protegidos con software de detección de virus. Esto debe realizarse antes de empezar a ejecutar o examinar a través de cualquier otro programa como por ejemplo un procesador de palabra.

99. Publicación de Material de la Empresa en el Internet

Política: Los usuarios no deben publicar material de la Empresa (software, memos internos, publicaciones de prensa, etc.) en ningún computador que tenga acceso público a Internet y que pertenezca al sistema, a menos que la publicación haya sido aprobada con anterioridad por el director de servicio al cliente.

100. Intercambio de Información en Internet

Política: Software, documentación y cualquier otro tipo de información interna de la Empresa no debe ser vendida o transferida a ninguna parte que no pertenezca a la Empresa, para ningún propósito diferente al del negocio expresamente autorizado la gerencia. No se debe dar el intercambio de software y/o datos entre la Empresa y una tercera parte a menos que se haya llegado a algún acuerdo escrito y éste haya sido firmado por el área encargada de Tecnologías de la información. Dicho acuerdo debe especificar tanto los términos del intercambio, como las formas en que el software y/o los datos deben ser manejados y protegidos.

101. Cargar Software a Otras Máquinas por medio de Internet

Política: Los usuarios no deben cargar software que haya sido licenciado por terceros, o software que haya sido desarrollado por la Empresa, a ningún computador a través de Internet a menos que se tenga una autorización previa del Director de la dependencia al que pertenece el usuario.

102. Actualizar Información de la Empresa a través de Internet

Política: Los usuarios que se conecten a los sistemas de la Empresa utilizando Internet no están autorizados a modificar directamente ninguna información de la Empresa.

103. Deshabilitar Java dentro del Web Browser de Internet

Política: Todos los usuarios de Internet deben desactivar Java cambiando la configuración original del software del browser de internet. Estas configuraciones se pueden cambiar únicamente cuando los usuarios visiten los webs de organizaciones conocidas y confiables, o cuando utilicen el Intranet de la Empresa.

104. La Ejecución del Programa Java está prohibido a menos que se haya Validado la Firma Digital

Política: Los colaboradores tienen prohibido ejecutar applets de Java bajados desde Internet, a menos que: a) el applet provenga de una fuente confiable y conocida, y b) la firma digital haya sido chequeada y no se haya descubierto ningún problema.

105. El Acceso a Internet utilizando los Computadores de la Empresa se debe hacer a través de un Firewall

Política: El acceso a Internet utilizando computadores en las oficinas de la Empresa está permitido cuando el usuario se comunica a través del firewall de la Empresa. Otras formas de acceso a Internet, como conexiones con modem con un proveedor de Internet (ISP), están prohibidas si se utilizan computadores de la Empresa.

XIV. CONEXIONES DE INTRANET

106. Solicitud de Permiso para Publicaciones en Intranet

Política: Antes de que cualquier información se publique en intranet de la Empresa, se deben obtener permiso por parte de la Dirección de Servicio al Cliente y del propietario de la información relacionada.

107. Todos los Contenidos publicados en Intranet son Propiedad de la Empresa

Política: A menos que se cuente con una aprobación por adelantado de la Dirección de Servicio al Cliente, y una nota explícita en la página de intranet en cuestión, todos los contenidos publicados en intranet de la Empresa son propiedad de la misma.

108. Chequeo previo a la Publicación de información en Intranet

Política: Antes de publicar material de la Empresa en Intranet, los colaboradores deben chequear a fondo toda la información y programas para asegurarse que no incluyan virus, caballos de Troya y cualquier otro código malicioso. Antes de publicar la información, los colaboradores también deben confirmar la actualidad, oportunidad y relevancia de la misma.

109. Los Desarrolladores de Sitios de Intranet deben utilizar la Guía de Imagen de la Empresa

Política: Todos los colaboradores que hagan desarrollos en intranet deben seguir los lineamientos de existentes de imagen corporativa y utilizar los recursos encontrados en el sitio de implementación de Intranet.

XV. REPORTE DE PROBLEMAS DE SEGURIDAD

110. Reporte Interno de Violaciones y Problemas en la Seguridad de la Información

Política: Los colaboradores de la Empresa tienen la tarea de reportar todas las violaciones y problemas con la seguridad de la información al área encargada de Tecnologías de la información en un tiempo prudente para que así se pueda tomar una acción que los solucione prontamente.

111. Centralización de los Reportes relacionados con Problemas en la Seguridad de la Información

Política: Todas las vulnerabilidades conocidas además de todas las violaciones evidenciadas deben ser comunicadas en forma rápida al área encargada de Tecnologías de la información. Adicionalmente, todas las revelaciones de información de la Empresa no autorizadas, deben ser reportadas a los propietarios de información involucrados. Está estrictamente prohibido reportar violaciones de seguridad, problemas o vulnerabilidad a cualquier parte fuera de la Empresa (exceptuando auditores externos) sin la previa aprobación escrita de la Dirección Jurídica.

112. Interferencia al Reporte de Problemas en la Seguridad de la Información

Política: Cualquier intento de interferir, prevenir, obstaculizar o disuadir a un miembro del personal en su esfuerzo por reportar posibles problemas o violaciones en la seguridad de la información está estrictamente prohibido y es causal de acciones disciplinarias. Cualquier forma de retaliación contra reportes individuales o investigaciones acerca de problemas o violaciones en la seguridad de la información también está prohibida y causa acción disciplinaria.

113. Reporte Externo de Violaciones en la Seguridad de la Información

Política: Si es requerido por la ley o regulaciones, la administración debe informar a las autoridades externas, lo más pronto posible, acerca de violaciones en la seguridad de la información. Si no existe este requerimiento, realizado en conjunto con las Direcciones Jurídica y de Control Interno, la administración debe sopesar las ventajas y desventajas de revelar externamente antes de reportar estas violaciones.

114. Reporte de Mal funcionamiento en el Software Requerido

Política: Todo el mal funcionamiento aparente en el software debe ser reportado inmediatamente al gerente en línea o al proveedor de servicios del sistema de información.

115. Investigación requerida en los Siguientes delitos de Computador

Política: Cuando se demuestren evidencias claras de que la Empresa ha sido victimizada por un delito de computador o comunicaciones, se debe llevar a cabo una investigación. Esta investigación debe proveer información suficiente para que el administrador pueda tomar pasos que aseguren que: a) Dichos incidentes no se puedan presentar nuevamente, y b) Se hayan restablecido medidas de seguridad efectivas.

116. Retención de Información acerca Violaciones en la Seguridad e Información de Problemas

Política: La información que describe todos los problemas de seguridad reportados y violaciones debe ser conservada por un período de tres años.

XVI. SELECCIÓN DE CONTROLES

117. Suministro de Hardware y Software únicamente a través de los canales de compra establecidos.

Política: Para garantizar conformidad con los estándares de seguridad de información propios, se debe conseguir todo el hardware y software a través de canales estándares de compra.

118. Utilización de la versión más actual del sistema operativo del computador.

Política: Para tomar ventaja de mejoras recientes de seguridad, después de una demora de algunos meses, la Empresa debe utilizar la versión más reciente de todos los sistemas operativos del computador multiusuario.

XVII. SELECCIÓN DE OTROS ASPECTOS DE CONTROL.

119. Acuerdos con terceras partes que manejan información de la Empresa.

Política: Todos los tratos de acuerdo con el manejo de información de la Empresa por terceras partes deben incluir una cláusula especial. Esta cláusula debe permitir que la Empresa audite los controles utilizados para esa actividad del manejo de la información, y que especifique la forma en la cual se protegerá la información de la Empresa.

XVIII. TERMINACIÓN Y DISCIPLINA

120. Medidas disciplinarias para la no aceptación de la seguridad de la información.

Política: El no cumplimiento con las políticas, estándares o procedimientos de seguridad informática, es la base para la terminación de acciones disciplinarias.

121. Medidas disciplinarias para varias violaciones de la seguridad de la información.

Política: Cuando se asume que la primera violación de las políticas de seguridad e informática es accidental o inadvertida, se debe hacer una amonestación. Una segunda violación sobre el mismo tema, hará que se envíe una carta al archivo del empleado. Una tercera violación, ocasionará la suspensión de trabajo por varios días sin pago. Una cuarta violación ocasionará el despido. Violaciones intencionales o a propósito sin importar el número de las mismas, puede resultar en acciones disciplinarias que deben llegar hasta el despido.

122. Remoción de información cuando se termina el empleo

Política: Hasta la culminación del contrato, los colaboradores no pueden retener o retirar desde las instalaciones de la Empresa cualquier información de la misma diferente a copias personales de correspondencia relacionada directamente con los términos y condiciones de su empleo. Cualquier otra información de la Empresa en custodia del trabajador que se retira, debe ser entregada al supervisor inmediato del trabajador en el momento de su salida.

123. Devolución de información por parte de contratistas, asesores y temporales.

Política: En la terminación o expiración de su contrato, todos los contratistas, asesores y temporales deben entregar personalmente a su administrador de proyectos todas las copias de la información recibida de la Empresa o creada durante la ejecución del contrato.

124. Responsabilidad por las acciones tomadas como respuesta a las cancelaciones laborales de colaboradores.

Política: En el evento en el que un empleado, asesor o contratista, se le termina su relación con la Empresa, el jefe inmediato del trabajador es responsable por: a) Asegurarse de que toda la propiedad en custodia del trabajador sea regresada antes de que el trabajador deje la Empresa, b) notificar a todos los responsables del manejo de las cuentas del computador y comunicaciones utilizadas por el trabajador tan pronto como se conozca su retiro y c) terminar todos los privilegios relacionados con el trabajo de la persona que se retira en el momento en que tiene lugar el mismo.

XIX. COPIAS DE SEGURIDAD Y CUSTODIA DE LA INFORMACIÓN.

125. Los administradores de TI de información no debe ser el dueño de la información.

Política: Con la excepción del computador operacional y de la información de la red, los administradores de Tecnologías de la Información no deben ser dueños de la información a cargo de los usuarios

126. Los usuarios son los dueños de la información corporativa procesada y almacenada en sus computadores.

Política: Cada usuario es dueño y responsable por la custodia de la información sensible que genera y tiene almacenada en su computador.

127. Los usuarios deben mantener debidamente organizada la información almacenada en sus computadores.

Política: Cada usuario es responsable por la correcta organización y clasificación en carpetas y subcarpetas, de los archivos en medios magnéticos que tiene a su cargo. No se deben guardar estos archivos en el ESCRITORIO de Windows, ni en ninguna de las carpetas estándar de Windows identificadas con los nombres de imágenes, documentos, música, video, etc. Estos archivos deben ser almacenados en las carpetas y subcarpetas creadas por cada usuario en el directorio raíz del disco duro de los

equipos asignados. No se deben guardar en los computadores de la entidad, archivos personales.

128. Copias de respaldo de la información almacenada en los computadores de usuarios

Política: Es responsabilidad del área encargada de Tecnologías de la información, la implementación de herramientas para realizar copias programadas de la información almacenada en los computadores de los usuarios **Se realizan Backups de la información financiera y administrativa diariamente y semanalmente se realizan Backups de la información sensible de cada área**. Así mismo, es responsabilidad de ésta área, la realización, validación y custodia de las copias de respaldo de la información que esté relacionada con la operación de la Empresa.

129. Repositorios de información en la nube (Dropbox, box, Google Drive, Ondrive, etc)

Política: La información sensible relacionada con las operaciones de la empresa, no debe ser almacenada en sitios públicos **gratis** en la nube, como son por ejemplo Dropbox, box, Google Drive, Ondrive, etc), debido a que esta información podría estar expuesta a accesos no autorizados. Solo pueden ser utilizados los sitios públicos corporativos en la nube que han sido autorizados previamente por el área encargada de Tecnologías de la Información.

130. Se requiere la designación de un custodio para todos los tipos principales de información

Política: Cada tipo principal de información debe tener un custodio designado. Cada custodio debe proteger apropiadamente la información de la Empresa manteniendo el control de acceso designado por el dueño, la sensibilidad de los datos y las instrucciones de los datos críticos.

131. Responsabilidades de seguridad de los custodios de la información.

Política: Los custodios de la información son responsables por la definición de procedimientos de control específicos, controles de acceso de la administración de la información, implementación y mantenimiento de las medidas de control de la información costo/beneficio, y suministrar capacidades de recuperación consistentes con las instrucciones de los dueños de la información.

132. Responsabilidades de seguridad de los usuarios de la información

Política: Todos los usuarios de la información de la Empresa deben cumplir con los requerimientos de control especificados por los dueños y/o custodios de la información. Los usuarios pueden ser colaboradores temporales, contratistas, asesores o terceras partes con quienes se hayan hecho arreglos especiales.

133. Protección de las copias de seguridad

Política: Las copias de seguridad de la información tanto de los usuarios como la de los servidores, deben estar encriptadas para evitar el riesgo de accesos no autorizados a esta información.

XX. SEGURIDAD FÍSICA

134. Control de acceso físico para áreas que contienen información sensitiva.

Política: El acceso a cada oficina, cuarto de computadores y área de trabajo que contiene información sensitiva, debe ser físicamente restringido. El Administrador responsable por el trabajo del personal del área técnica o directivos en esas áreas debe consultar al área encargada de tecnologías de la información para determinar el método de control apropiado de acceso (recepcionistas, chapas de llave metálica, chapas de tarjeta magnética, etc.).

135. Computadores multiusuario o sistemas de comunicaciones en cuartos asegurados.

Política: Todos los computadores multiusuario (servidores) y los equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir alteraciones y usos no autorizados.

136. Guardas o recepcionistas para áreas que contienen información sensitiva.

Política: El acceso a las oficinas de la Empresa por parte de visitantes u otras personas a áreas que contengan computadoras y otras áreas de trabajo que contengan información sensible debe estar controlada por guardas, recepcionistas u otras personas del área técnica o directiva. A los visitantes y demás no se les debe permitir el uso de las entradas de los colaboradores u otras vías de acceso no controladas a áreas que contienen información sensitiva.

137. No permitir ingreso de personas externas a través de puertas controladas.

Política: Los controles de acceso físicos para los edificios de la Empresa se hacen con la intención de restringir la entrada de personal no autorizado. Los colaboradores no deben permitir que personas no autorizadas o desconocidas pasen a través de puertas, compuertas y otras entradas a áreas restringidas al mismo tiempo que personas autorizadas acceden por esas entradas. Esto puede parecer rudo inicialmente, pero es esencial que sea mantenido por todos los colaboradores para la seguridad de la Empresa.

138. Se requiere seguridad física o encriptación para toda la información sensible.

Política: Todos los medios de almacenamiento de información (tales como discos duros externos, cintas magnéticas, y CD-rom's) que contengan información sensitiva deben estar asegurados físicamente cuando no se estén utilizando. Se hará una excepción si esta información es protegida vía un sistema de encriptación aprobado por el área encargada de las tecnologías de la información.

XXI. REGISTRO DE ACCESO A LAS INSTALACIONES.

139. Mantenimiento de registros del sistema de control de acceso a edificios.

Política: Para facilitar la evacuación y para sustentar investigaciones, la Dirección de Gestión Humana y Administrativa debe mantener registros del personal actual y el que ingresó previamente a las instalaciones de la Empresa. Esta información debe guardarse y ser retenida por al menos tres meses.

140. Cambio de códigos de control de acceso físico cuando se retiran colaboradores.

Política: En el evento de que un trabajador esté terminando su relación con la Empresa, todos los códigos de acceso de seguridad físicos conocidos por el trabajador se deben cambiar o desactivar.

141. Medidas de seguridad física para sistemas de comunicaciones y de computadores.

Política: Edificios que contengan computadores o sistemas de comunicación de la Empresa, deben ser protegidos con medidas de seguridad físicas que previenen que personas no autorizadas puedan obtener acceso a él. En el caso de los computadores portátiles, deben estar asegurados con guayas.

XXII. LOCALIZACIÓN DEL COMPUTADOR E INSTALACIONES DE LA CONSTRUCCIÓN.

142. Construcción adecuada para centros de cómputo o de comunicaciones.

Política: Los centros de comunicaciones y de computadores nuevos o remodelados de la Empresa, deben se construidos de tal forma que sean protegidos contra el fuego daño de agua, vandalismo, y otras amenazas que se conocen que puedan llegar a ocurrir, o que están cerca de ocurrir en los lugares involucrados.

143. Localización dentro de un edificio de las facilidades de comunicaciones y del computador.

Política: Para minimizar el robo y el daño por inundación, los computadores multiusuario y las instalaciones de comunicación deben estar localizados encima de la primera planta de los edificios. Para minimizar el daño potencial de humo y fuego las instalaciones de cocina deben ser localizadas lejos de los centros de cómputo. Igualmente para minimizar el daño potencial de agua, las instalaciones de los baños no deben estar localizadas directamente arriba de esos sistemas. Para minimizar el daño potencial de bombas y para minimizar el espionaje y la interferencia electromagnética no autorizada, estos sistemas no deben estar ubicados junto a un muro exterior de la Empresa.

144. Material combustible en los Centros de cómputo.

Política: Dentro de los cuartos de cómputo no deben almacenarse elementos con material combustible, ni se deben utilizar los centros de cómputo como bodegas para almacenar elementos.

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**DESCRIPCION DEL CAMBIO**	**OBSERVACIONES**
o	15-Sept-15	Versión inicial	No Aplica
1	29-Jul-16	Se define del periodo con que se realizan los Backups de la información de la empresa.	Se da cierre a una no conformidad.
2	11-Agos-16	Cambio Imagen Corporativa	No Aplica
3	12-Junio-18	Actualizado de acuerdo a la Guía PDE-G001	No Aplica

Elaboró	**Revisó**	**Aprobó**
Nombre: Marisol Alvarado Castillo Cargo: Directora Área: Dirección de Gestión Humana y Administrativa Firma: _____ Nombre: Myriam López M. Cargo: Profesional de Apoyo Área: Dirección de Planeación Firma: _____	Nombre: Sandra Milena Ruiz Cargo: Coordinador de Calidad Área: Dirección de Planeación Firma: _____ Nombre: Manuel Sandoval V. Cargo: Director de Planeación Firma: _____	Nombre: Marisol Alvarado Castillo Cargo: Directora de Gestión Humana y Administrativa Firma: _____