ADMINISTRACION
CONTROL
SEGURIDAD
EN
TECNOLOGIA INFORMATICA

ELECTRIFICADORA DEL HUILA S.A. ESP

MANUAL DE POLITICAS

Neiva, Huila,

POLITICAS DE SEGURIDAD INFORMÁTICA

Las políticas son la base fundamental de todo esfuerzo enfocado a la seguridad de la información. Con el fin de ser efectivo, el proceso para fortalecer la seguridad de la información debe tener un conjunto de políticas que brinden instrucciones claras y establezcan el soporte de la alta gerencia. Las políticas son usadas como punto de referencia para un sinnúmero de actividades relacionadas con la seguridad de la información tales como: Diseño de controles en los sistemas de información, controles de acceso, análisis de riesgos, investigaciones de fraude por los sistemas de información, y sanciones disciplinarias de trabajadores por violaciones en la seguridad.

Como las políticas de seguridad tienen un impacto muy alto en la organización, es muy importante que estas sean claras, concisas y que respondan al ambiente donde se pretenden implementar. Las políticas deben ser revisadas periódicamente para asegurar su aplicabilidad en la organización.

SEGURIDAD LÓGICA

1. Longitud mínima de la clave.

Política: La longitud de la clave debe ser mínima de ocho (8) 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 adivinar.

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, acrónimos comunes y jerga común.

3. Prohibición de utilizar palabras claves cíclicas

Política: Los usuarios no deben construir palabras claves compuestas por caracteres que no cambian o combinadas con cierto número de caracteres que cambian predeciblemente. Es decir, que no se deben utilizar caracteres que típicamente cambian tal como el mes, un departamento, un proyecto o algún otro factor que fácilmente puede adivinarse (por ejemplo. "X34ENE" en Enero, "X34FEB" en Febrero, etc.).

4. Uso de palabras claves repetidas

Política: Los usuarios no deben construir palabras claves que sean idénticas o muy similares a palabras claves utilizadas anteriormente.

5. Palabras claves con caracteres alfabéticos y no alfabéticos

Política: Todas las palabras claves deben tener al menos un carácter alfabético y uno no alfabético; se consideran caracteres no alfabéticos los números y los signos de puntuación, no se deben utilizar caracteres de control y otros caracteres no impresos porque involuntariamente pueden causar problemas de transmisión en la red o sin intención llamar ciertos servicios del sistema.

6. Palabras claves con letras mayúsculas y minúsculas

Política: Todas las palabras claves escogidas por el usuario deben tener al menos un carácter alfabético en minúscula y otro en mayúscula. Esto ayudará para que las palabras claves sean más difíciles de adivinar por personas no autorizadas o por espías industriales.

DISEÑO DE INTERFACES DE PASSWORD DE USUARIOS DEL SISTEMA

14. Visualización de palabras claves

Política: Las palabras claves en pantalla o impresas no se deben presentar, esto con el fin de evitar que personas no autorizadas las puedan observar o recuperarlas.

15. 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 treinta (NN) días.

16. Cambio obligatorio de palabras clave al accesar 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.

17. Límite de intentos consecutivos infructuosos para ingresar la palabra clave

Política: Después de tres intentos consecutivos e infructuosos de ingreso de la palabra clave, el sistema debe: (a) suspender el acceso del usuario hasta que el administrador del sistema lo ponga a funcionar de nuevo, (b) incapacitarlo temporalmente por no menos de tres minutos, o (c) si hay algunas otras conexiones o discado externos de la red desconectarlos.

18. Proceso de identificación personal ante el sistema

Política: En el momento en que el usuario va a ingresar a la red y/o al sistema del computador, se le debe solicitar una combinación de la identificación (user-ID) y de una palabra clave. La identificación del usuario debe enviarse completamente a otros computadores, sistemas de manejo de base de datos y aplicaciones.

DISEÑO DE PASSWORD INTERNOS DEL SISTEMA

19. Passwords ilegibles en estaciones de trabajo externas.

Política: Los passwords fijos nunca deben estar en forma legible fuera de la Empresa en estaciones de trabajo.

20. Protección de palabras claves enviadas a través del correo

Política: Si las palabras claves se envían por correo regular o sistemas físicos de distribución similares, éstas se deben enviar separadamente de las del usuario IDs. Estos correos no deben tener ninguna marca indicando la naturaleza del contenido. También se deben ocultar dentro de un sobre en papel oscuro que no revele fácilmente su contenido.

22. Encripción de palabras claves

Política: Las palabras claves siempre deben estar encriptadas cuando se almacenen por cualquier período de tiempo significativo o cuando sean transmitidas por las redes. Lo anterior evitará que sean descubiertas por interceptores de líneas telefónicas o telegráficas, personal técnico que lea los sistemas de log`s u otras partes no autorizadas.

23. Incorporación de palabras claves dentro del software

Política: Las palabras claves no se deben incorporar dentro de los programas de software, esto para que las claves se puedan cambiar en el momento que sea necesario.

24. Diseño de sistemas para evitar la recuperación de las palabras claves

Política: Los computadores y sistemas de comunicación deben ser diseñados, probados y controlados de forma que se prevenga la recuperación de palabras claves almacenadas, ya sea que aparezcan encriptadas o no.

25. Confianza del usuario para operar el sistema en el proceso de autenticación

Política: Los Desarrolladores de Sistemas de Aplicación deben confiar en los controles de acceso y las palabras claves proporcionadas por el sistema para su operación o por un paquete de control de acceso que lo enlace con el sistema operativo. Los Desarrolladores de Sistemas no deben construir otros mecanismos separados para coleccionar passwords o códigos de identificación de usuarios; igualmente, no deben construir o instalar otros mecanismos para identificar o autenticar la id empresa de los usuarios sin un permiso del Administrador de Seguridad de información corporativa.

26. Control de acceso al sistema con palabras individuales para cada usuario

Política: El sistema de control de acceso al computador y al sistema de comunicación se debe realizar por medio de palabras claves únicas para cada usuario, es decir que no se admite el acceso a archivos, base de datos, computadores y otros recursos del sistema por medio de palabras claves compartidas.

28. Cambio de códigos claves proporcionados por el fabricante (palabras default)

Política: Todas las palabras claves de fábrica proporcionadas por el fabricante se deben cambiar antes que la empresa utilice cualquier sistema de computación o de comunicaciones para sus negocios.

PASSWORD RELACIONADO CON LAS RESPONSABILIDADES DEL USUARIO

29. 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.

30. Permiso para usar la misma palabra clave en diferentes sistemas

Política: Los usuarios deben abstenerse de utilizar el mismo código o palabra clave en múltiples sistemas de computación de la empresa.

31. 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.

32. Cambios de palabras o códigos claves después del mantenimiento a un computador o un sistema de información.

Política: Cuando un sistema del computador multi-usuario emplea palabras o códigos claves fijos como su mecanismo de control de acceso principal, éstos se deben cambiar inmediatamente finalice el mantenimiento.

33. Escribir palabras claves (passwords) y dejarlas en donde otros pueden descubrirlas.

Política: No se deben escribir passwords y dejarlos en lugares donde personas no autorizadas pueden descubrirlos.

34. Escribir passwords usando técnicas secretas.

Política: Los usuarios no deben escribir sus passwords al menos que: (1) ellos hayan realmente ocultado estos passwords en un número de teléfono o con otros caracteres aparentemente no relacionados, o (2) que ellos hayan usado un sistema de código para ocultar el password.

35. Prohibición de passwords compartido

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.

36. 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. Asimismo, se les prohibe a los usuarios que realicen cualquier actividad con códigos de identificación de usuario que pertenezcan a otros usuarios (exceptuando user-IDs anónimo como “Huésped”)

PASSWORD RELACIONADOS CON LAS RESPONSABILIDADES DEL ADMINISTRADOR

37. Cambio forzoso de todos los password

Política: Siempre que un sistema ha sido atendido por partes no autorizadas, los administradores del sistema deben cambiar inmediatamente cada password en el sistema. Incluso si sospechan además de un arreglo se requiere que todos los password se cambien inmediatamente. En cualquiera de estas circunstancias, una versión verdadera del manejo del sistema y de todo el software relacionado con seguridad debe también volverse a cambiar. Así mismo bajo ninguna de estas circunstancias, todos los cambios recientes al usuario y privilegios del sistema deben revisarse para modificaciones no autorizadas.

38. Acreditación personal de Id empresa para obtener un password

Política: Los passwords nunca deben descubrirse por medio de líneas telefónicas habladas. Para obtener un nuevo password o para cambiarlo, un usuario debe presentarse en persona y acreditar la identificación adecuada.

39. User-ID y password requerido para conectarse al computador de la red

Política: Todos los usuarios deben tener su id empresa verificada con un user-Id y un password -- o por otros medios que proporcionen una seguridad igual o mayor antes de permitirles usar computadores de la Empresa conectados a una red.

40. Log-Off de los computadores personales conectados a las redes

Política: Si los computadores personales (PCs) están conectados a una red, cuando no estén en uso deben siempre estar log-Off.

CONTROL DE PRIVILEGIOS

USO DE LOS SISTEMAS

41. No se deben almacenar juegos ni usar los sistemas del computador de la empresa para estas actividades.

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

42. 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 los negocios de la empresa. Se permite su uso para fines personales únicamente en los horarios que la empresa ha destinado.

43. Prohibición contra los usos no aprobados del sistema

Política: Los suscriptores de los servicios de computación y comunicación de la Empresa no deben usar estas facilidades para asuntos comerciales personales , venta de productos o bien para comprometerse en otras actividades comerciales que no sean aquellas expresamente permitidas por la la empresa.

44. Prohibición del uso del Internet con fines personales

Política: El uso de sistemas de información de la empresa para tener acceso al Internet con fines personales no será tolerado y puede considerarse causa para una acción disciplinaria. Todos los usuarios del Internet deben estar enterados que estas pruebas pueden dar lugar a auditoria detallada del log que refleje transmisiones.

45. Uso personal de las facilidades del internet de la empresa solamente en las horas libres

Política: La administración de la Empresa estimula a los empleados a que exploren el Internet, pero 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, juegos, 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.

46. Usos permitidos de información de la empresa

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

47. 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 no sean empleados, contratistas, o consultores para usar los computadores de la empresa, o de los sistemas de comunicación, a menos que primero se obtengan la aprobación por escrito de la subgerencia respectiva

48. 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 inmediatamente después de que el trabajador cesa de prestar sus servicios a la Empresa.

49. Responsabilidad por daño a información y a programas por negligencia

Política: La Empresa usa controles de acceso y otras medidas de seguridad para proteger la veracidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos, la administración debe tener la autoridad para: (1) restringir o derogar cualquiera de los privilegios del usuario, (2) inspeccionar, copiar, remover, o bien alterar algún dato, programa, u otro sistema que pueda socavar estos objetivos, y (3) tomar cualquier otra acción que estime necesaria para manejar y proteger sus sistemas de información. Esta autoridad puede emplearse con o sin notificación a los usuarios. La Empresa desconoce cualquier responsabilidad por pérdida o daño a la información o software que resulte de sus esfuerzos para lograr estos objetivos de seguridad.

50. El acceso no autorizado por medio de los sistemas de información de la empresa.

Política: Se prohibe a los trabajadores que usen los sistemas de información de la Empresa para tener acceso no autorizado a cualquier otro de los sistemas de información o de cualquier forma dañar, alterar, las operaciones de estos sistemas. Del mismo modo se les prohibe capturar o de otra forma obtener palabras claves, claves encriptadas o cualquier otro mecanismo de control de acceso que pueda permitirles un acceso no autorizado.

ADMINISTRACIÓN DE CONTROL DE ACCESO A LA INFORMACIÓN

51. Controles de acceso al sistema del computador

Política: Toda la información del computador principal que sea sensible, crítica o valiosa debe tener controles de acceso al sistema para garantizar que no sea inapropiadamente descubierta, modificada, borrada.

52. Restricción privilegiada basada en la necesidad de su labor

Política: El computador y los privilegios del sistema de comunicación de todos los usuarios, sistemas, y programas deben ser restringidos basados en la necesidad del desempeño de sus funciones.

53. Códigos de identificación de usuarios que identifiquen únicamente a un usuario en particular

Política: Cada computador o sistema de comunicaciones debe únicamente identificar uno y solamente un código de identificación por usuario. Códigos de identificación de usuario para grupos o que sean compartidos no son permitidos.

54. Prohibición de Usuarios-IDs genéricos basados en funciones del cargo

Política: Se prohíbe tener usuarios IDs genéricos basados en sus funciones de trabajo. En cambio, usuarios-IDs deben únicamente identificar individuos específicos.

55. Prohibición del reutilización de códigos de identificación de usuario

Política: Cada código de identificación de usuario debe ser único y solamente habilitarse con el código de usuario que le ha sido asignado. Después que un funcionario se retira de la empresa, no debe volver a usarse ninguno de los códigos asignados anteriormente.

PRIVILEGIOS ESPECIALES

56. Restricción de privilegios especiales del sistema

Política: Los privilegios especiales del sistema, tales como la habilidad de examinar los archivos de otros usuarios, debe restringirse a aquellos que sean directamente responsables del manejo y/o seguridad del sistema. Estos privilegios deben otorgarse solamente a aquellos personas que han tenido y aprobado entrenamiento especial.

57. Aprobaciones requeridas para la creación de usuario-ID y asignación privilegiada

Política: A usuarios específicos se les puede otorgar usuarios IDs solamente cuando tienen aprobación por anticipado del supervisor inmediato. Antes de dar a estos usuarios la aplicación comercial de privilegios del sistema ésta debe ser aprobada por el propietario de la información

58. Usuarios-IDs inactivos y revocaciones del privilegio automático

Política: Todos los usuarios-IDs deben automáticamente revocar los privilegios asociados después de un período de treinta (30) días de inactividad.

59. Gestión inapropiada y revocación de privilegios de acceso

Política: La administración de la empresa se reserva el derecho de revocar los privilegios de cualquier usuario en cualquier momento.

60. Prohibición para probar controles de información del sistema

Política: Los trabajadores no deben comprobar, o intentar arreglar controles internos, a menos que anticipadamente y por escrito hayan sido específicamente aprobados por el administrador del sistema

61. Limitaciones de funcionalidad para poderosas herramientas de los sistemas de información

Política: Todas las herramientas de los sistemas de información, construidas o distribuidas por la empresa, que puedan usarse para causar un daño significativo deben ser automáticamente restringidas para que sean solamente usadas en el(los) propósito(s) determinado(s).

62. Privilegios para modificar la información comercial en el ambiente de producción.

Política: Restringir el uso de los privilegios únicamente a los trabajadores responsables de la administración para la modificación de la informaciónl de la Empresa en el ambiente de producción.

63. Proceso controlado para modificación de la información en el ambiente de producción.

Política: Establecer privilegios para que los usuarios del sistema puedan modificar información en producción en formas predefinidas, para preservar la integridad de la información y ejecutándose en forma controlada.

64. Actualización de la Información comercial en producción

Política: Definir privilegios del sistema para que el personal que no pertenezca al usuario final responsable (auditores internos, administradores de seguridad de información, programadores, operarios del computador, etc.) no se les permita modificar directamente los datos de información comercial en el ambiente de producción.

65. Privilegios del personal técnico y cambio de los parámetros de control en los sistemas en producción

Política: Los operadores del computador no deben tener acceso a modificar los datos y programas en producción, al igual que la funcionalidad del sistema.

ACTIVIDADES ADMINISTRATIVAS

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

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

69. Administración para todos los computadores de la red.

Política: Las configuraciones y parámetros instituidos para todos los equipos adscritos a la red de la Empresa, deben ser ejecutadas por la oficina de sistemas.

.

70. Transferencia de las tareas una vez el funcionario deja su cargo.

Política: Cuando un funcionario deja su cargo con la Empresa, tanto los archivos magnéticos como los de papeles, los debe recibir el jefe inmediato, para determinar a quién se los asigna, delegando específicamente la responsabilidad sobre ellos.

71. Borrado de archivos después que el funcionario se retira.

Política: cuatro (4) semanas después que un funcionario ha dejado permanentemente la Empresa, todos los archivos guardados en los directorios del usuario serán depurados.

INFORMACIÓN A INCLUIR EN LOS ARCHIVOS DE LOGS

72. Logs en los sistemas de aplicación que contengan Información sensitiva

Política: Todos los sistemas de aplicación en producción que contengan información sensitiva de la Empresa deben generar Logs que indiquen cada adición, modificación, borrado y divulgación de esta información.

73. Información que se sospecha como crimen informático o abuso del Computador.

Política: Para proporcionar evidencia en investigaciones y tomar acciones administrativas y de carácter legal, se debe obtener la información necesaria de, los archivos de seguridad “Logs”, los estados del sistema actual y las copias de los archivos (back-up) y de todos los demás potencialmente involucrados, cuando se sospecha que ha ocurrido un crimen informático o abuso en el computador. La información debe custodiarse hasta el momento en que estime conveniente o determine la Alta Dirección de la Empresa.

VIRUS INFORMÁTICO

74. Los usuarios no deben intentar erradicar virus del computador

Política: Si los usuarios sospechan que hay infección por un virus, ellos deben inmediatamente parar de usar el computador, desconectarlo de todas las redes y llamar al encargado solicitando ayuda.

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

Política: Se prohibe a los usuarios finales eliminar virus informáticos de los sistemas de la empresa, cuando éstos sistemas 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 la oficina de sistemas.

76. Prohibición para bajar y cargar Software de Internet, en los sistemas corporativos por parte de terceras personas

Política: Los trabajadores 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, Troyanos y otro software que puede dañar la información y los programas en producción.

77. Pruebas de virus antes de usar los programas en la empresa

Política: Para prevenir la infección por virus en los computadores, los trabajadores 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 la oficina de sistemas.

78. 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 la oficina de sistemas.

79. Programas de chequeo de integridad del sistema para computadores personales

Política: Para detectar oportunamente y prevenir la expansión de virus informáticos, todos los computadores personales y los servidores LAN de la empresa, se les debe correr un software de chequeo de integridad. Este software detecta cambios en la configuración de los archivos, en los archivos de software del sistema, en los archivos de software de aplicación y en otros recursos del sistema. El software de chequeo de integridad debe ser continuamente activado o correrse diariamente.

80. Se requieren instalar programas de chequeo de virus en PCs y servidores LAN

Política: la oficina de sistemas debe contar con programas automáticos para examinar virus e instalarlo y ejecutarlo continuamente en todos los servidores de red de área local (LAN) y en los diferentes computadores personales que se conectan a la red institucional.

81. Copias de respaldo al software original para microcomputadores

Política: Todos el software del microcomputador 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, si no que deben reservarse para cuando se presenten infecciones de virus, daños en el disco duro y otros problemas en los microcomputadores.

82. Los usuarios del sistema no deben incluir virus en el software

Política: Los usuarios del sistema no deberán escribir, generar, compilar, copiar, propagar, ejecutar, o intentar introducir intencionalmente cualquier código a la computadora, que haya sido diseñado para causar daño o impedir la normal actuación de la memoria de la máquina, archivos de datos o programas, sistemas operativos o software aplicativo. Estos programas nocivos son conocidos como virus.

TÉCNICAS Y HERRAMIENTAS DE DESARROLLO

83. No ejecutar pruebas al software con información confidencial

Política: No es permitido ejecutar pruebas al software aplicativo con datos o información real del ambiente de producción.

84. Documentar la ocurrencia de errores y las acciones a seguir para el software desarrollado.

Política: Todo software que se desarrolle o personalice en la empresa y que produzca resultados no esperados, siempre deberá producir mensajes de error y las acciones a seguir por parte del usuario deberán documentarse.

85. Todo desarrollo de software debe tener requerimientos formales

Política: Se deberán definir previamente las especificaciones o requerimientos formales para todo desarrollo de software. Estas especificaciones deberán ser parte integral de un acuerdo entre los dueños de la información involucrada y los programadores del software. El acuerdo deberá ser completado y aprobado antes de comenzar el desarrollo o personalización del código del sistema.

86. Eliminación todas las rutas de acceso no autorizadas en los ambientes de producción

Política: Antes de trasladar al ambiente de producción el software desarrollado, los programadores o personal técnico de informática deberán eliminar todas las rutas de acceso especiales o privilegiadas, para que solamente puedan ser obtenidas de acuerdo con los procedimientos corporativos normales de seguridad. Todos los privilegios de usuarios especiales que se concedieron para el desarrollo del software no deberán ser permitidos en el ambiente de producción.

87. Utilización técnicas y herramientas de desarrollo probadas y confiables

Política: Para todo desarrollo de software se deberán utilizar técnicas y herramientas de desarrollo conocidas en el mercado local del que se tenga certeza que su comportamiento es seguro y confiable.

88. Uso de lenguajes de programación de alto nivel

Política: Utilizar lenguajes de programación de últimas generaciones para reducir el volumen de código a desarrollar, la dificultad de mantenimiento del software, el tiempo exigido para desarrollar una aplicación, y el número de fallas.

89. Documentación estandarizada para toda la tecnología que se encuentre en el ambiente de producción

Política: Cada usuario que desarrolle o implemente software o hardware para ser usado por la empresa en las actividades propias del negocio, deberá documentar el sistema de acuerdo con el avance de la Implementación. La documentación deberá ser escrita para que el sistema pueda ser

utilizado por personas no familiarizadas con él. La documentación deberá cubrir usuarios finales operativos y técnicos.

90. La utilización del hardware y software de pruebas o de diagnóstico

Política: El hardware y software de diagnóstico, como el de monitoreo de líneas de comunicación, sólo deberán ser usados por personal autorizado con propósitos de prueba y desarrollo. El Acceso a esta clase de hardware y software deberá controlarse estrictamente por la oficina de sistemas.

91. Los ambientes de producción, desarrollo y pruebas

Política: El Nuevo software de aplicación en desarrollo o personalización deberá guardarse estrictamente separado del que se encuentra en producción y del respectivo de pruebas. Si las facilidades existentes lo permiten, la separación de los ambientes deberá hacerse en equipos de cómputo independientes. Si no se deberán separar los directorios y librerías, y hacer cumplir estrictamente los controles automáticos de acceso a los usuarios.

92. Restricción del acceso a la información de los aplicativos en producción al personal de desarrollo de software.

Política: El acceso a la información de producción no deberá permitirse al personal de desarrollo de Software de aplicación, excepto cuando se trate de información de producción que este directamente relacionada con el software de la aplicación particular que se esté trabajando, actividad que deberá ser supervisada por el Jefe de la oficina de sistemas.

PROCESO DE CONTROL DE CAMBIOS

93. Todos los sistemas automáticos que se encuentren en producción deberán cumplir con el procedimiento formal de control de cambios.

Política: Para todos los equipos de cómputo y sistemas de comunicación utilizados en procesos de producción en la empresa, se deberá aplicar un procedimiento formal de control de cambios que garantice que sólo se realicen los cambios autorizados. Este procedimiento de control de cambios deberá ser aplicado al software, hardware, comunicaciones, interfaces y a los procedimientos.

94. Prohibición a los usuarios finales de la instalación de software en sus equipos o computadoras personales

Política: Los usuarios finales no deberán instalar software en sus computadoras personales sin que medie la autorización de la oficina de sistemas.

95. Documentación sobre los cambios hechos a los sistemas en producción.

Política: La documentación que refleja todos los cambios hechos sobre los equipos de producción, deberán prepararse simultáneamente con el proceso de cambio. Esta documentación deberá contemplar las propuestas de cambio, la aprobación de la dirección, y la manera como el cambio fue realizado. (diseñar protocolo)

96. Documentación de los procesos para el entrenamiento y operación de los sistemas en producción

Política: Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento y operación adecuados.

97. Todo software que ha sido primero probado externamente por terceros también debe ser probado por la empresa

Política: Programas ejecutables (código objeto de software) provistos por empresaes externas, deberán probarse por la empresa antes de la instalación en el ambiente de producción. La lista de instrucciones de programa (código fuente de software) provisto por empresaes externas deberá ser revisado y probado en cuanto a sus compilaciones y los programas ejecutables por el equipo de trabajo asignado por la oficina de sistemas., antes de su instalación en producción.

98. El traslado del software del ambiente de desarrollo al de producción

Política: El personal de desarrollo de aplicaciones de la empresa, no deberá estar habilitado para trasladar cualquier tipo de software al ambiente de producción.

99. Todo software adquirido a través de un proveedor deberá someterse al proceso de control de cambios de la empresa

Política: Antes de comenzar a instalarse, nuevas o diferentes versiones del sistema operativo y el relacionado con el software de los sistemas en producción, deberá ser validado primero por el proceso de control de cambios establecido en la Empresa.

100. Revisiones periódicas a los sistemas operativos del ambiente de producción

Política: Revisiones periódicas a los sistemas operativos del ambiente de producción deberán ejecutarse para asegurar que únicamente los cambios autorizados han sido realizados y no otros.

101. Los mantenimientos al software deberán realizarse únicamente sobre el código fuente.

Política: Todos los cambios permanentes al software en producción deberán hacerse con el código fuente.

102. Todo software que se incorpore a producción debe tener su propio plan de contingencia

Política: Siempre que se pase al ambiente de producción un nuevo software o uno significativamente modificado, se requieren procedimientos contingentes especiales para evitar considerables pérdidas en la empresa. La administración del aplicativo deberá preparar un plan de contingencia de conversión que refleje las diferentes formas o maneras de asegurar la continuidad del servicio a los usuarios que potencialmente se puedan ver afectados

PARTICIPACIÓN DE GRUPOS DE TERCEROS

103. Todo el software usado en actividades críticas del negocio debe ser custodiado.

1)**Política:** Si un software de terceros está siendo considerado, y éste se usará en una actividad crítica de la empresa, una de las dos siguientes condiciones deberá quedar consignada en el contrato de adquisición. La primera es que el proveedor externo entregue la licencia del código fuente a la empresa en caso de presentarse una e las siguientes condiciones A. Caso fortuito o fuerza mayor que impida la prestación del servicio B. Declaratoria de quiebra o liquidación forzosa de la firma C. Decisión unilateral del oferente de no continuar prestando el soporte técnico, mantenimiento y actualización del software ofrecido.Esta **Política** permitirá a la empresa poder continuar con el mantenimiento del software aunque el proveedor haya salido del mercado o pueda haberse discontinuado el producto o se presente negligencia en términos de arreglar los problemas detectados en el programa fuente.

104 Se instalará en los equipos únicamente el software ejecutable

Política: Para prevenir copias de software no autorizadas y el empleo de la propiedad intelectual, todo el software desarrollado por la empresa para ser usado por sus clientes, , y otros terceros, deberá ser distribuido únicamente el código objeto.

105.**Todo acuerdo con terceros para utilizar el software de la empresa debe ser formal**

Política: Para prevenir el uso no autorizado, del software desarrollado por la empresa por parte de los clientes, y otros terceros, deberá distribuirse sólo después de que los destinatarios hayan cumplido con los procedimientos de permisos por parte de las subgerencias respectivas.

OPERACIÓN DEL COMPUTADOR

106. Se prohibe fumar, comer y beber en el centro de cómputo e instalaciones con equipos tecnológicos

Política: Todos los empleados y visitantes no deberán fumar, comer o beber en el centro de cómputo o instalaciones con equipos tecnológicos. Al hacerlo estarían exponiendo los equipos a daños eléctricos, así como a riesgos de contaminación sobre los dispositivos de almacenamiento de datos.

SEGURIDAD DE LOS DATOS

DERECHOS DE PROPIEDAD INTELECTUAL

107. 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 las normas, políticas y procedimientos relacionados con los Sistemas de Información.

108. Los trabajadores deberán conceder a la empresa, exclusividad sobre los derechos de propiedad intelectual de sus desarrollos.

Política: Todos los derechos de propiedad intelectual de los productos desarrollados o modificados, por los empleados de la institución, durante el tiempo que dure su relación laboral son de propiedad exclusiva de la Empresa.

109. 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 trabajadores , consultores, proveedores o contratistas para el beneficio y uso Corporativo, es propiedad exclusiva de la Empresa.

110. 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.

111. Reintegro de los recursos suministrados por la empresa para el desarrollo de trabajos.

Política: Los empleados temporales, 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.

PROTECCIÓN DE LOS DERECHOS DE PROPIEDAD INTELECTUAL

112. Todo software institucional y su documentación deberá tener un aviso sobre los derechos de autor y propiedad literaria.

Política: Todo el software y la documentación que posea la empresa deberán incluir avisos de los derechos de autor y propiedad literaria.

113. Revisiones periódicas a los contratos de licenciamiento de software.

Política: Los contratos de licenciamiento de Software, se deberán ser revisados periódicamente, por la unidad usuaria responsable en la Empresa, en el cumplimiento de los compromisos asumidos por las partes.

114. 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.

115. Todo proveedor corporativo debe estar inscrito en un registro de control institucional.

Política: Todos los productos de hardware y software adquiridos por la empresa, deberán ser registrados por Proveedor. Para asegurar que el soporte y los descuentos en actualización de versiones sean obtenidos con facilidad.

116. Adquirir las licencias de software necesarias para desarrollar las actividades corporativas.

Política: La Oficina de Sistemas deberá solicitar la compra de licencias de software de uso generalizado adicionales, para los casos en que los trabajadores las soliciten.

117. No es permitido hacer copias del software sin autorización escrita del proveedor

Política: Ningún Software corporativo deberá copiarse a menos que sea previamente autorizado por el proveedor, en el contrato de compra, o las copias que se realicen sean para propósitos de apoyar el Plan de Contingencia corporativo.

CONFIDENCIALIDAD DE LOS DATOS

POLÍTICAS GENERALES PARA LA CONFIDENCIALIDAD DE LOS DATOS

118. Acuerdos de confidencialidad para todos los trabajadores de la Empresa.

Política: Todos los empleados, consultores, contratistas y personal temporal deben firmar un acuerdo de confidencialidad de la información al iniciar su trabajo con la Empresa.

DERECHO A CONOCER

119. Divulgación de las Políticas de seguridad y procedimientos

Política: Como regla general, la información de políticas de seguridad y procedimientos se deben revelar únicamente a trabajadores de la empresa y a entes externos seleccionados (ejm. auditores).

120. Ubicación y naturaleza de información confidencial de la empresa

Política: La información acerca de la naturaleza y localización de la información, tal como la ubicación en el diccionario de datos, es confidencial y únicamente se debe ser divulgada por quienes estén autorizados.

DISEÑO DE LOS SISTEMAS

121. Establecer una meta cuantificable en cuanto a la disponibilidad del sistema

Política: Los sistemas de computación críticos deben ser evaluados frecuentemente en cuanto a su disponibilidad, los usuarios deben poder accesar los sistemas de computación compartidos al menos en un 96% del tiempo en horas normales de trabajo, tomando como base el tiempo de uso del sistema en un mes de trabajo.

PLANES DE CONTINGENCIA

122.Clasificar en forma anual las aplicaciones de acuerdo con su nivel de criticidad.

Política : En conjunto con los usuarios mas experimentados, la Oficina de Sistemas deberá realizar periódicamente una revisión del grado de criticidad de las aplicaciones en producción. Este proceso de clasificación permitirá llevar acabo un plan de contingencia coordinado y organizado

.

123. Preparación y mantenimiento de un plan de respuesta a emergencias de sistemas de información (Sistemas Alternos).

Política : Para los sistemas de Cómputo y comunicaciones, la administración de la empresa debe preparar, actualizar periódicamente y regularmente probar el plan de emergencia. Estos planes deben asegurar la continuidad de las operaciones críticas del negocio en el evento de una interrupción o degradación del servicio.

124. Entrenamiento cruzado para el Staff técnico crítico

Política: En todo momento deben existir por lo menos dos miembros del staff técnico en capacidad de cumplir con las tareas de un cargo técnico crítico, si menos de dos personas en la compañía pueden cumplir con esta política, se debe en forma inmediata elaborar un plan de capacitación o contratación de outsourcing o cualquier otra alternativa para lograr tener dos personas técnicas capacitadas en cargos críticos.

125. Preparación y mantenimiento de un plan de recuperación de desastres en sistemas de cómputo e información

Política : La administración de la empresa debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, huracán, terrorismo, inundación o maremotos.

126. Proceso del plan de continuidad de computadores y del negocio

Política : El Oficina de Sistemas debe documentar y mantener para toda la empresa un proceso estándar para el desarrollo y mantenimiento del plan de contingencia para computadores

127. Inventario anual de recursos de computación hardware y software, etc.

Política : El Oficina de Sistemas debe preparar un inventario anual de los sistemas de información en producción, de tal forma que puedan ser rápidamente restablecidos en el caso de un desastre. El inventario debe incluir todo el hardware, software y canales de comunicación de datos existentes.

128. Mantenimiento preventivo en los sistemas de comunicaciones y computadores

Política : Se debe realizar en forma regular un mantenimiento preventivo a los sistemas de comunicación y computadores, de tal forma que el riesgo de fallas sea mantenido en una probabilidad baja.

129. **Números telefónicos de los trabajadores del Oficina de Sistemas**

Política : Todos los miembros del Oficina de Sistemas deben mantener informados a sus jefes inmediatos donde puedan ser localizados en caso de ausencias sin importar su causa. Esta política garantiza que todos los miembros del Oficina de Sistemas este siempre disponible en caso de emergencias y/o desastres.

BACK-UP, ALMACENAMIENTO DE ARCHIVOS Y DISPOSICION DE LOS DATOS

130. Que datos se deben respaldar y con que frecuencia

Política : Toda la información de valor, confidencial y crítica de la empresa, debe ser periódicamente respaldado en medio magnético. Este proceso de respaldo debe ser realizado al menos mensualmente.

131. Respaldos periódicos y complementarios requeridos para computadores portátiles

Política : Los usuarios que usen computadores portátiles deben hacer respaldo de su información crítica ante de ser llevados fuera del lugar de trabajo, Estos respaldos deben permanecer en el sitio de trabajo y deben ser hechos en forma adicional a los procedimientos de respaldo preestablecidos.

132. Encripción de los datos de respaldo que se archiven en sitios fuera de la empresa

Política : Toda información de valor, confidencial o crítica que sea respaldada y almacenada en un lugar externo a la empresa debe ser respaldada en forma encriptada para prevenir que esta sea divulgada o usada en forma no autorizada por otras empresaes o personas.

133. Deben existir por lo menos dos copias de respaldo de la información de valor, confidencial o crítica de la empresa.

Política : Todos los usuarios son responsables de realizar una copia de respaldo del original de la información de valor, confidencial o crítica a su cargo. Estas copias separadas deben ser hechas cada vez que un número significativo de cambios sean hechos a la información.

134. Las copias de respaldo de la información crítica de la empresa deben ser custodiadas en forma externa

Política : Al una copia reciente completa (no increméntales) de la información crítica de la empresa deben ser almacenados en forma externa.

135. Proceso de revisión de los backups de usuario final por parte de las áreas administrativas

Política : Los jefes de cada área o sus delegados deben asegurar que se haga un backup de la información sensible, de valor y crítica contenida en los microcomputadores (PC), estaciones de trabajo u otros sistemas menores.

136. Especificaciones y frecuencia del proceso backup

Política : Se deben llevar a cabo backups increméntales de toda la información de los usuarios finales diariamente de los días laborales por parte del administrador de backups. Un backup total de toda la información con una periodicidad semanal.

137. Backup automático en los servidores de área local

Política : Todos los usuarios que tengan conectados sus computadores a la red local, deben dejar prendidos sus computadores (no_login) de tal forma que se pueda hacer un backup automático.

138. Los trabajadores de tipo administrativo

Política : Los trabajadores responsables de cada área administrativa deben identificar y mantener una lista completa de los registros vitales de su área en caso de un proceso de restauración después de un desastre.

139. Prueba regular de la calidad de los backup

Política : El backup de información de valor, sensible o crítica que esté almacenada por largos periodos de tiempo, debe ser validada en forma anual de tal forma que se pueda garantizar que no ha sufrido ningún deterioro.

140. Prueba regular de los dispositivos para hacer backup de información

Política : Los dispositivos electrónicos usados para hacer backup de información de valor, sensible o crítica debe ser de alta calidad y probados regularmente para garantizar que cumplan su objetivo de respaldo de la información establecida. Dispositivos que no garanticen esta calidad, no deben ser usados para hacer copias de información para recuperación.

INTEGRIDAD DE LOS DATOS

CONOCIMIENTO Y "STATUS" DE INTEGRIDAD

141. Informar a la administración en caso de falla de los controles de integridad

Política : Si los controles de integridad fallan o se sospecha de alguna anomalía con estos, la administración debe ser informada inmediatamente y anexar un informe completo del caso.

142. Todas las transacciones que ingresen a un sistema de producción computarizado deben estar debidamente autorizadas

Política : Deben existir procedimientos para garantizar que toda entrada de datos a un sistema de producción computarizado haya sido debidamente autorizado.

SEGURIDAD EN COMUNICACIONES

ESTABLECIMIENTO DE LOS SISTEMAS Y DE LAS RUTAS DE ACCESO

143. 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, redes de valor agregado, Internet y otros, deben ser protegidos por mecanismos de control de acceso aprobados por el oficina de sistemas. Está política no aplica para computadores que usen modems para conectarsen en forma de terminales de salida a otros sistemas.

144. La red de amplia cobertura geográfica debe estar separada en diferentes dominios

Política : La red de amplia cobertura geográfica departamental / nivel nacional debe estar dividida en forma lógica por diferentes dominios, cada uno separado con controles de seguridad perimetral y mecanismos de control de acceso.

.

145. 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 , debe pasar a través de un punto adicional de control como : firewall, servidor de acceso o gateway.

146. 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.

147. Conexiones directas entre los computadores de la empresa y otras organizaciones requieren de un mecanismo de Tunneling

Política : La conexión directa entre un computador de la empresa y otra organización vía redes públicas de datos como Internet requieren de la aprobación del oficina de sistemas, quienes estipularan los mecanismos de seguridad apropiados como Firewalls y Tunneling.

CREACION DE CONEXIONES EN REDES

148. Autorización previa para la intercomunicación directa entre computadores de la empresa

Política : Conexión en tiempo real entre dos o más computadores de la red interna de la empresa debe ser explícitamente aprobada por el oficina de sistemas con el fin de evitar la omisión de controles de acceso lógico.

149. 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. La empresa 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.

150. Uso de los computadores de los empleados para realizar funciones de la empresa

Política : El uso de los computadores, software, periféricos e información de los empleados para realizar funciones de la empresa, debe ser autorizado por la dirección de cada área administrativa.

SISTEMAS DE CORREO ELECTRONICO

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

Política: Los trabajadores 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.

152. Usuarios no deben Emplear el Sistema de Correo Electrónico como una Base de Datos

Política: Los usuarios deben regularmente cambiar información importante de archivos de mensajes de correo electrónico a un documento de procesador de palabra, base de datos y otros archivos. Los sistemas de correo electrónico no están intencionados para guardar archivos de información importante. Mensajes de correo electrónico guardado pueden ser periódicamente destruidos por administradores de sistemas, erróneamente borrado por los usuarios y de otras maneras pueden perdercen cuando existen problemas en el sistema.

154. 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 el comité del programa institucional.