POLÍTICA DE USUARIO SOBRE LA SEGURIDAD DE INFORMACIÓN EL MANEJO DE EQUIPOS DE CÓMPUTO

1. Introducción

El uso compartido y el intercambio de información con nuestros clientes, socios y entre nuestros compañeros de trabajo constituyen una base esencial para lograr las metas de la empresa. La Información tiene que ser considerados uno los valores de nuestra empresa, que tiene que ser igual de protegido.

Mal funcionamiento, pérdida de información, robo o espionaje son contradictorias a nuestro tema central, y representan, sólo teniendo en cuenta la posible pérdida de confianza de nuestros clientes, socios y compañeros de trabajo, una amenaza potencial ITICPE S.A.C. La Protección de la información debe, por lo tanto, garantizarse en todos los procesos de negocio y proyectos de los clientes, en el que se procesa la información o el apoyo de la información y la comunicación, la tecnología. De este modo, las leyes nacionales e internacionales y los reglamentos tienen que ser respetadas.

La Seguridad de la información sólo se puede lograr, si todos los usuarios de la información y la comunicación cumplen ciertas reglas básicas.

2. Objetivo / Meta del Documento

Esta norma sobre seguridad de la información constituye directrices vinculantes para el uso / aplicación de la información y / o técnicas de comunicación, equipos / sistemas.

2.1 Ámbito de aplicación del Documento

Toda la empresa

2.2 Grupo objetivo del documento

Todos los empleados ITICPE S.A.C. que hagan uso de dispositivos / sistemas basados en la información y / o tecnología de la comunicación. Todo el personal ejecutivo ITICPE S.A.C., que tienen una función ejemplar en lo que respecta a la adhesión de la guía y que son responsables de la puesta en práctica en su área. Además, todos los compañeros de trabajo y externos a las organizaciones de servicios, que proporcionan servicios de TI dentro de ITICPE S.A.C.

2.3 Responsabilidad del Documento

La Gerencia General es el último designado y responsable de esta norma de seguridad de TI.

Para contribuir a la aplicación, realización y mantenimiento de las medidas de seguridad el Gerente General es responsable de la dirección profesional de los mecanismos de apoyo, de tomar el liderato y acciones disciplinarias. Los incidentes serán reportados de inmediato con el fin de coordinar las iniciativas de seguridad.

2.4 Bases para el documento

La Norma de Gestión de TI de Seguridad de la ITICPE S.A.C se basa en las normas DIN ISO/IEC 27001:2008 Sistema de Gestión de Seguridad de la Información y la especificación de la norma DIN ISO / IEC 27002:2008 Código de Prácticas para la Gestión de Seguridad de la Información.

La idoneidad y la eficiencia operativa de las medidas necesarias para la protección de los valores de información, así como la viabilidad y aplicabilidad son los temas centrales de esta norma.

3. Definiciones

Comunicación segura y datos de la red de ITICPE S.A.C

La “Seguridad" de la red del ITICPE S.A.C abarca todos los dispositivos de información y comunicación como teléfonos móviles, un servidor, notebooks, PC impresoras y componentes de red, que están bajo el control y/o ejercicio de cualquier influencia de ITICPE S.A.C. También incluye componentes de alquiler o de otra manera, directa o exclusivamente por ITICPE S.A.C.

En el momento, la “seguridad" de la red abarca todo el mundo, aproximadamente 400 sitios que están conectados entre sí y con la sede corporativa a través de las líneas de comunicación.

Redes públicas:

Todos los demás componentes de la tecnología de la información pertenecen a la "inseguridad", la red pública, que está bajo el control de potencialmente no confiable personas u organizaciones.

"Las redes públicas" son, entre otras cosas:

- El Internet, utilizado por muchos millones de personas en todo el mundo, en la que los servicios como WWW, e-mail, chat y muchas otras cosas, se puede utilizar. El Internet no está sujeto a ninguna norma de seguridad. Por ejemplo, tampoco hay garantía de que los correos electrónicos a través de Internet llegan a sus destinatarios. Además, existe el riesgo de que los correos electrónicos son leídos por terceros.
- Online-Servicie por compañías como T-Online, AOL, etc., que también permiten el acceso a Internet
- Las cadenas de radio, por ejemplo, puntos de acceso denominada con "Wireless LAN"-tecnología redes de telefonía móvil.

La "seguridad" de la red de ITICPE S.A.C está conectado a Internet en los puntos definidos con dispositivos de seguridad adecuados ("firewalls"). Los dispositivos de seguridad deberán impedir el acceso no permitidos desde Internet a los "asegurados" de la red de ITICPE S.A.C

4. Normas a seguir

Las siguientes reglas deben ser seguidas por todas las empresas de ITICPE S.A.C.

4.1 Normas generales para el uso de dispositivos y redes de información y comunicación-Tecnología

Todos los cambios físicos y lógicos y el mejoramiento de los "asegurados" de ITICPE S.A.C referidos a la comunicación y red de datos, se realizan exclusivamente bajo la administración de la Gerencia General. En consecuencia, los usuarios finales o el personal de TI local no puede añadir o modificar componentes de la LAN o WAN o la creación de redes inalámbricas (WLAN) por su cuenta.

La conexión de los dispositivos privados a la red "segura" no está permitida.

Los visitantes externos, por ejemplo, consultores, tienen que utilizar sus propias tecnologías inalámbricas (por ejemplo, UMTS-cards) o - cuando esté disponible - una red especial para los huéspedes, que permite el acceso a los recursos públicos solamente. Ellos no pueden conectar sus dispositivos a los "asegurados" de la red. Las personas externas que trabajan en proyectos o contratos en los sitios del acceso de ITICPE S.A.C tienen que contar con los permisos de la Gerencia General.

La Gerencia General puede realizar una auditoría de seguridad en cualquier momento también sin previo aviso.

La carga o la ejecución de datos y/o programas de Internet pueden generar una gran cantidad de problemas de seguridad, como son las más conocidas como los virus, troyanos y rootkits, que a menudo tratan de robar información personal o de la empresa. Los usuarios no deben confiar en el hecho de que los datos o los programas descargados, provienen de fuentes confiables.

Únicamente personal autorizado y el Jefe de Calidad, puede bajar a su equipo SW libre para el manejo de estadísticas u otra información.

Está prohibido usar software descargado de la internet a fin de garantizar la integridad de la información.

Se prohíbe a los compañeros de trabajo de ITICPE S.A.C, almacenar los datos de la empresa, en dispositivos no aprobados, discos duros u otros sistemas de almacenamiento de datos.

4.2 Uso de dispositivos para la comunicación Empresarial y de TI

Los dispositivos de negocios que ITICPE S.A.C ofrece al empleado para su uso, son propiedad de la empresa y están sujetas a ciertas condiciones de uso.

- Los PCs de trabajo (desktops, notebooks y otros dispositivos de TI) están disponibles para los empleados exclusivamente para el uso en los negocios de ITICPE S.A.C. Cualquier forma de uso privado o de otro tipo está prohibido, a menos que se apruebe en un acuerdo explicito o, en alguno casos, por escrito por el Gerente General.
- En las oficinas todas las funciones de seguridad existentes tienen que ser activadas y utilizadas. Por ejemplo, al salir del lugar de trabajo, la PC debe ser automáticamente bloqueada después de un máximo de 15 min. Como alternativa el bloqueo puede ser activado manualmente.
- Al dejar el lugar de trabajo, se debe tener cuidado de tener las medidas de seguridad necesarias para evitar el acceso de personas no autorizadas a la información de la empresa.
- Las PCs de escritorio tienen que ser mantenidas bloqueadas y en los sitios de trabajo definidos.
- No se permite hacer modificación a las configuraciones preestablecidas o instalación de software adicional en la PC de la empresa a menos que esta haya sido aprobada por la Gerencia General.
- Si los intentos de manipulación por parte de un usuario pueden ser probados o si el usuario aplica las herramientas posibles para eludir los mecanismos de seguridad instalados, ITICPE

S.A.C puede recurrir a instancias legales laborales como medidas de sanción.

- El usuario no puede realizar ningún cambio en el hardware.
- En todos los PCs de negocios deben contar con los programas antivirus y firewalls.

4.2.1 Uso de la Comunicación-y dispositivos informáticos en las oficinas

Mientras no esté ocupada la oficina las ventanas y las puertas que dan al exterior (balcones, patios) tienen que permanecer cerradas.

Las puertas de las habitaciones no ocupadas, en el que se encuentra el equipo, los documentos confidenciales, soportes de datos o de TI, tiene que estar cerradas. Esto impide el acceso por personas no autorizadas.

El cierre de oficinas individuales es especialmente importante si se encuentran en las zonas donde hay tráfico de público o su acceso no se puede controlar por otros medios.

En casos como por ejemplo en oficinas abiertas, en el que la oficina no puede ser bloqueada, cada empleado tiene que proteger su/sus documentos ("Política de escritorios limpios") antes de dejar el sitio de trabajo y asegurar su espacio personal (por ejemplo su escritorio, armario).

Durante cortos períodos de ausencia, mientras que el equipo está encendido, se debe bloquear el equipo si no se puede cerrar la oficina y continuar con el uso de la computadora sólo es posible sólo después de introducir una contraseña.

Los dispositivos antirrobo tienen que ser aplicados en todas partes, donde los valores tienen que ser protegidos u otras medidas, por ejemplo control de accesos al área, no pueden ser aplicados, especialmente en el caso de laptops o dispositivos móviles.

Si el PC es utilizado por diferentes usuarios y si los usuarios tienen diferentes derechos de acceso a los datos o programas en la PC, la seguridad requerida a través de control de acceso sólo se puede obtener, si cada usuario cierra la sesión en el PC después de haber cumplido su trabajo o al salir del lugar de trabajo.

4.2.2 El uso de dispositivos fuera de los sitios ITIC

El uso de computadores portátiles y PC`s de escritorio en el hogar con acceso a los datos de ITICPE S.A.C estará debidamente autorizado a un círculo controlado de personas. El almacenamiento local de datos en los dispositivos y el uso de conexiones públicas con la red de datos de ITIC representan un riesgo para la propiedad, los procesos, los datos y los aspectos económicos relevantes de la empresa.

Los discos duros locales de estos dispositivos, por lo tanto, tienen que ser encriptados por medios adecuados. Las especificaciones y recomendaciones de la organización de TI regionales tienen que mantenerse o ser considerados, respectivamente.

Durante el acceso remoto a través de redes no seguras que hay que asegurarse de que de inicio de sesión es segura y los datos transferidos estén debidamente encriptados.

4.2.3 Uso de dispositivos de comunicación móviles y de IT

Los dispositivos móviles, tienen que ser mantenidos bajo la responsabilidad de la persona a la que se le asigna; si un empleado actúa sin tener en cuenta las políticas recomendaciones de uso y salvaguardia la empresa se reserva el derecho de determinar las medidas disciplinarias pertinentes.

Los dispositivos no deben ser guardados en el auto; en caso y solo por razones justificadas, se tenga que dejar el dispositivo en el auto por un corto tiempo, este no debe ser visible de fuera del auto.

Los dispositivos deben ser protegidos de temperaturas extremas y de alguna influencia ambiental que le pueda causar daño.

4.2.4 El uso de ordenadores no protegidos (por ejemplo, ordenadores privados, cafés Internet, hoteles)

El uso de los ordenadores privados, los ordenadores de los cibercafés y hoteles con fines comerciales se debe limitar a las necesidades urgentes. Los empleados no están autorizados para guardar datos que se supone que no son públicos, en los medios de comunicación de datos, disco duro o de otro tipo, no autorizados.

4.2.5 El uso de las palabras clave (password)

Comunicaciones y sistemas de TI, tienen que ser protegidos mediante la asignación de una palabra secreta personal (el llamado código o contraseña). La contraseña (s) tienen que ser mantenidas en secreto.

Las contraseñas no se pueden transmitir a sus compañeros de trabajo, supervisores u otras personas. La contraseña debe ser cambiada regularmente, por lo menos cada 180 días. Tiene que ser cambiado de inmediato, si hay alguna

sospecha de que se conoce a otra persona. Las palabras de código asignado por el administrador del sistema durante la configuración inicial tienen que ser cambiado inmediatamente después del primer uso.

Las palabras de código no pueden ser fácil "adivinar" y deben tener un mínimo de 8 caracteres.

Un mínimo de 3 de cada 4 diferentes tipos de personajes se debe mezclar:

• mensajes pequeños (A. Z)

• Las letras mayúsculas (A. Z)

• Números (0 ... 9)

• Los caracteres especiales (“! /()#*"...)

Deben evitarse:

- Nombres, nombres especialmente el inglés, y el segundo de la misma persona o de miembros de la familia, los cumpleaños, las placas y las unidades de organización, así como las palabras triviales como el código 12345678
- Las palabras comunes de la lengua nacional o en el vocabulario de inglés
- Nombres comerciales famosos
- Basta con contar la cantidad al final de la contraseña, e. g. Julia01, etc. Julia02

Palabras del código personales no pueden ser almacenadas en forma escrita cerca de la PC y no se guardará en el disco duro del PC.

Es imprescindible para evitar sofocar las palabras clave personal por escrito. Si en ciertos casos existe la necesidad de anotar las palabras código, esta nota debe mantenerse en un sobre cerrado y con el almacenamiento en un armario seguro.

4.2.6 Los medios de almacenamiento

Todos los soportes de datos, datos qué se pueden copiar a partir de una PC, se consideran medios de almacenamiento (por ejemplo, disquetes, CD o DVD), así como los aparatos electrónicos (por ejemplo, USB de almacenamiento, reproductor de MP3, tarjetas de memoria, por ejemplo, en cámaras digitales, disco duro externo. etc.)

Si los medios de almacenamiento con datos que no se supone que son públicos se utilizan fuera de las oficinas o centros de cómputo de ITICPE S.A.C, estos tienen que ser codificados con los medios adecuados.

4.3 Reglamento de Organización

4.3.1 en casos de incidentes de seguridad (Gestión de Incidentes de Seguridad)

En los casos de sospecha de virus, troyanos, spyware u ocurrencia de otros posibles incidentes de seguridad del departamento tiene que ser notificado de inmediato.

4.3.2 Asignación y conservación de los derechos de acceso

Normas básicas sobre la asignación y mantenimiento de los derechos de acceso:

- La administración del acceso sólo podrá ser realizada por una persona autorizada y sólo en el marco de las normas establecidas en la política de control de acceso correcta (TRASA)
- En principio, sólo la cantidad de accesos pueden ser asignados, según se requiera para el desempeño de la tarea.
- Cada usuario será capaz de buscar sus derechos dentro de una determinada aplicación, así como cada uno responsable de su área.
- Los cambios personales y relacionados con las tareas tienen que ser considerados de inmediato dentro de la administración el derecho de acceso.
- En caso de un empleado es retirado de la empresa, su código y los derechos asociados tienen que ser desactivados y / o eliminados de inmediato.
- En intervalos regulares (por lo menos una vez al año) la búsqueda de "identificaciones muertas", es decir, las identificaciones que no se hayan utilizado durante un período, el sistema relacionado con lo anterior período definido se tiene que realizar.

4.3.3 Reglamento de Organización de las posibilidades de acceso en casos de sustitución o de emergencia, respectivamente,

Los acuerdos tienen que ser hechos, en caso de emergencia debido a la ausencia de un empleado (por ejemplo, vacaciones o enfermedad), que permiten su acceso deben ser verificados.

En las aplicaciones y los sistemas de TI, un reemplazo de la regulación en general deberá ser proporcionado, para evitar la necesidad de revelar las contraseñas en los casos de ausencia.

Después de regresar el usuario tiene que ser informado de la divulgación de la contraseña y le pedirá que seleccione una nueva

contraseña. Además, la divulgación y la duración tienen que ser documentado.

Dependiendo de la viabilidad técnica "de un solo uso de contraseñas" o las contraseñas limitadas puede ser asignado.

4.3.4 Directrices para el intercambio de datos con terceros

En caso de intercambio regular de datos con terceros, se debe establecer las reglas específicas o acuerdos entre las partes.

En esa directriz / acuerdo de los siguientes temas que se abordarán:

- Especificación de los responsables
- Nombramiento de los contactos (en temas de índole técnica, organizativa y de seguridad)
- La no divulgación-acuerdo
- Especificación de los datos, el uso de Las aplicaciones y formatos de datos que se deben utilizar
- Pruebas de virus
- Eliminación de los datos
- Regulación de la gestión de claves, si es necesario
- El cumplimiento de las regulaciones legales pertinentes

4.3.5 El aumento de la conciencia de seguridad informática

La seguridad informática sólo puede garantizarse si todos los participantes, las personas afectadas, poseen el nivel apropiado de conocimientos en seguridad de TI, general y especialmente sobre los riesgos y medidas a adoptar en sus propias áreas de trabajo. La responsabilidad recae en la Dirección para proporcionar el presupuesto necesario, con medidas de formación adecuada.

4.4 Uso de software y servicios de comunicación

4.4.1 Instalación, configuración y desinstalación de software

El Software se puede instalar, configurar y desinstalar exclusivamente por los empleados o personal autorizado. Se deben tomar las medidas adecuadas para prevenir la pérdida de datos en caso de fallo durante la instalación.

4.4.2 gestión de licencias y de control de versiones de software estándar

Sólo el software con licencia puede ser ejecutado en el sistema, salvo autorización de uso de SW libre por parte de algunos empleados de la empresa.

Los administradores y usuarios de los diferentes sistemas de TI, por lo tanto, tienen que asegurarse de que no se utiliza el software sin la correspondiente licencia.

4.4.3 Uso-Prohibición para los no aprobados por Software

Para asegurarse de que no hay programas con efectos indeseables en ejecución y que el sistema no se utiliza fuera del alcance definido del funcionamiento de una manera incontrolada, la instalación de software no autorizado está prohibido y – en la medida de lo técnicamente posible -.

Para ello, se debe considerar:

- Las excepciones sólo se permiten con un permiso especial de la correspondiente del GG.
- Tiene que estar documentado, que las versiones de los archivos ejecutables del programa fueron aprobadas.
- Los programas aprobados tienen que ser controlados regularmente en materia de seguridad relacionados con las actualizaciones.

4.4.4 Protección contra virus

Las siguientes reglas sobre la protección frente a virus, troyanos y rootkits que tener en cuenta:

- Todos los sistemas de PC que cuentan con programas de protección contra virus.
- Los datos de origen desconocido o con características poco comunes no pueden ser ejecutados o abiertos respectivamente.
- E-mails que contienen remitentes sospechosos, las líneas de asunto, o textos deben ser tratadas con precaución.
- Si los archivos adjuntos sospechosos con contenido ejecutable se han abierto, estos casos deben ser reportados al gerente de la empresa.
- Cada soporte de datos externo o que se utiliza externamente (por ejemplo, disquetes, CD, DVD, memorias USB, discos duros externos) tienen que ser escaneados en los antivirus antes de su uso.
- Cada portador de datos tiene que ser revisado por completo.

- Después del uso, los soportes de datos tienen que ser removido de las unidades.
- detección de virus de los archivos cifrados es la responsabilidad del usuario.
- Si un virus de ataque ha sido detectado, el PC se apaga de inmediato y la línea tiene que ponerse en contacto con el virus de la eliminación-.

4.4.5 Normas sobre el uso del correo electrónico y otros servicios de comunicación

Esta regla se aplica al uso del correo electrónico y servicios de comunicación como la mensajería instantánea (chat), el uso de los foros, blogs, almacenamiento de datos de Internet y servicios similares, a través del cual la información de negocios puede ser el intercambio o transmisión.

Por lo tanto, los siguientes puntos deben ser considerados:

- Para fines de negocios sólo el sistema de correo electrónico que ha sido programado debe ser utilizado exclusivamente, salvo autorizaciones de excepción.
- La transferencia de datos, que se supone que no son públicas, a través de otros servicios de comunicación o de los proveedores de Internet no está permitido.
- Envío de correos electrónicos a otros servicios de correo electrónico - especialmente las cuentas privadas de correo electrónico - no está permitido. Las excepciones tienen que ser aprobados.
- Direccionamiento de los mensajes de correo electrónico tiene que ser clara, sin ambigüedad, para evitar la entrega incorrecta.
- En caso de enviar información confidencial vía correo electrónico, el e-mail tiene que ser codificado.
- Para todos los correos electrónicos de negocios relevantes para los destinatarios externos, una firma (la información del remitente al final del mail) debe ser utilizado.
- La línea del asunto del sistema de comunicación siempre debe ser completada.
- Los correos electrónicos no deben ser almacenados innecesariamente en la bandeja de entrada.

5 excepciones

Excepciones a las reglas postuladas sólo están permitidas con la aprobación expresa de la persona responsable de información correspondiente y debe ser documentado.

6. mantenimiento de los equipos de cómputo:

Todos los equipos usados por la empresa deben ser sometidos a rutinas de mantenimiento preventivo mínimo cada doce meses, el mantenimiento correctivo debe hacerse inmediatamente para prevenir la perdida de los datos.

Las actividades de mantenimiento deben hacerse por parte de personal debidamente seleccionado.

7. Copias de seguridad de la información:

Toda la información considerada pertinente y sensible, debe contar con una copia de respaldo, bien sea en los servidores o en medios de almacenamiento debidamente autorizados.

NOTA FINAL:

1. Este documento forma parte del SGC y su manual, no requiere autorizaciones adicionales;
2. El mismo obedece a las directrices de ITICPE S.A.C y a su aplicación vinculante a ITICPE S.A.C;