POLÍTICA DE SEGURIDAD INFORMÁTICA
PAZ CORP. S.A.

Tema	:	Política de Seguridad Informática Paz Corp. S.A.
Área Responsable	:	Gerencia de Tecnología
Fecha Elaboración	:	16 de octubre de 2015
Elaborado por	:	César Sepúlveda Firma:
Revisado por	:	Boris Staropolsky Firma: BORIS STAROPOLSKY FURSZYFER Firmado digitalmente por BORIS STAROPOLSKY FURSZYFER Fecha: 2023.03.31 17:26:50 -03'00'
Aprobado por	:	César Barros Firma:
Fecha de Actualización	:	Miércoles, 1 de Marzo de 2023
Nombre del archivo	:	Política de Seguridad Informática Paz Corp. S.A.

I. OBJETIVO

El presente documento tiene por objetivo individualizar a cada usuario dentro de la red corporativa, esto a su vez permite administrar de forma correcta los accesos a servicios y recursos dentro de la red respetando la seguridad de la información y protegiendo la integridad de los datos, activo fundamental de la organización.

II. ALCANCE

El contenido de este procedimiento aplica a todos los trabajadores de la Compañía.

III. RESPONSABILIDADES

Los responsables de su utilización y ejecución recaerán directamente en cada área y sus integrantes.

IV. DESCRIPCIÓN DEL PROCEDIMIENTO

1. Seguridad de la Red

Objetivo: Cada usuario de la red sea identificado y autenticado en forma separada para poder acceder a los recursos del sistema.

1.1. Todo usuario de la red de la empresa, debe ser autenticado mediante al menos un nombre de usuario (username) y una contraseña (password). A cada funcionario de la empresa se le prohíbe compartir o revelar su identificación personal o contraseña a otros.

Al personal de la empresa se le prohíbe conectarse a algún sistema sin el nombre de usuario que le ha sido asignado, o permitir que otras personas utilicen su identificación para conectarse a algún sistema que se realice con la identificación de usuario que le fue asignada.

1.2. Las contraseñas asignadas por la empresa a un empleado deben ser cambiadas por éste la primera vez que se conecta. Las contraseñas:

1.2.1. Deben consistir en un mínimo de ocho caracteres de extensión y deben estar constituidas por caracteres alfanuméricos (números, letras y caracteres especiales)
1.2.2. Deben ser cambiadas al menos cada dos meses.
1.2.3. Deben ser cambiadas de inmediato si el usuario cree que la contraseña ha trascendido.
1.2.4. Nunca deben escribirse en lugar visible.

1.2.5. No deben reutilizarse una vez cambiadas. De acuerdo con las políticas de la empresa, el sistema guarda un histórico de 5 registros.

1.2.6. Debe ser cambiada de inmediato si el usuario advierte actividad sospechosa o anormal en su computadora.

1.2.7. Debe mantenerse en forma confidencial y nunca debe ser compartida o divulgada con los demás.

1.3. Ante licencias médicas continuas de 15 o más días u otro tipo de ausencia prolongada, el área de Tecnología, a solicitud de la Jefatura Directa, bloqueará las claves de los sistemas de la Empresa, sean estos: correo corporativo, SAP, Fiori u otro, evitando un eventual mal uso de dichas claves y usuarios por parte de terceras personas. Cuando el Colaborador se reincorpore, deberá solicitar el desbloqueo al área de Soporte.

1.4. Si un usuario deja de ocupar su computador durante 15 minutos, el sistema en forma automática cargará el protector de pantalla bloqueando su sesión y le solicitará nuevamente su contraseña para ingresar.

1.5. Está estrictamente prohibido el uso de equipos personales, computacionales o de impresión, para desempeñar labores profesionales dentro de la red de PazCorp La empresa no se hará responsable por daños o pérdidas relacionadas con estos equipos. Del mismo modo, queda absolutamente prohibido conectar tales equipos a la red computacional corporativa, por el riesgo de seguridad y confidencialidad de la información de PazCorp y la vulnerabilidad de estas políticas.

2. Uso de Internet

Objetivo: El personal de PazCorp utilice internet exclusivamente como herramienta de trabajo asociada a sus labores sin exponer la seguridad de la información de la empresa.

2.1. Se prohíbe expresamente visitar sitios no relacionados con los negocios de PazCorp o las funciones que para cada cargo han sido definidas.

2.2. Se prohíbe expresamente descargar o copiar cualquier software de Internet, aun cuando el software o aplicación sea gratis o de libre disposición (freeware).

2.3. El uso de Internet dentro de la red computacional de PazCorp es de exclusivo uso laboral y no de uso personal.

El área de TI controlará y administrará los accesos a Internet mediante software especializado con el fin de asegurar el rendimiento y seguridad de la red computacional de PazCorp.

2.4. Los usuarios no deben suscribirse a listas de distribución de correo electrónico sin previa autorización de PazCorp.

Esto incluye horóscopos, noticias por correo, y otros. Constituye una amenaza importante a la seguridad de los sistemas de la Empresa.

3. Correo Electrónico

Objetivo: El personal utilice el correo electrónico corporativo de manera eficaz y apropiada a sus funciones y labores.

3.1. Se prohíbe a los empleados usar el correo de la empresa para enviar o reenviar e-mail o correos electrónicos en cadena, ofensivos, correos considerados "spam", de carácter racial, político, religioso o sexual, ya sea dentro o fuera de la empresa.

3.2. El uso de e-mail corporativo para asuntos personales está permitido siempre y cuando su uso no incluya alguno de los casos indicados en el párrafo anterior y no altere el normal funcionamiento de este servicio al interior de la empresa.

3.3. La empresa se reserva el derecho de intervenir, controlar y denegar cualquier transmisión de e-mail corporativo mediante los sistemas de seguridad que posea en cualquier caso que considere afectada la seguridad o el normal funcionamiento de su servicio de correo o cuando la acción del usuario pueda ser constitutiva de delito.

3.4. Se prohíbe transferir datos o información confidencial y/o estratégica de la Empresa, o almacenada en los quipos de la Empresa a casillas de correo personal, privado o cualquier otro correo no autorizado previamente por escrito..

3.5. No se debe abrir ningún mensaje procedente de direcciones de correo desconocidas. Se recomienda que este tipo de e-mail sean eliminados en forma inmediata.

3.6. No se debe enviar nunca por correo nombre de usuario y/o contraseñas, códigos de alarmas, combinación de caja fuerte o cualquier otra información que se utilice para dar acceso a oficinas, sistemas, bienes o servicios de la empresa.

3.7. Todo e-mail enviado (saliente) debe especificar de qué se trata en el espacio designado como "Asunto" o "Subject", esto porque podría ser catalogado como correo "spam" y no llegar a destino.

3.8. Se prohíbe el uso de cuentas de e-mail privadas o personales para tratar asuntos laborales o del negocio de PazCorp.

3.9. Los usuarios no podrán enviar correos electrónicos de más de 20 Mb. Adicionalmente, queda estrictamente prohibido enviar por email archivos de música, videos, fotografías y cualquier tipo de adjunto no relacionado con las funciones específicas del empleado o del negocio de PazCorp.

3.10. Será responsabilidad de cada empleado anunciar sus ausencias en caso de licencia médica, vacaciones, viajes o cualquier otro motivo a través de la opción "Ausente de Oficina" de Outlook o el sistema de correos que esté utilizando PazCorp al momento de la ausencia, dejando establecido en dicha respuesta el correo de la(s) persona(s) que atenderá(n) los requerimientos mientras el Colaborador se encuentra fuera de oficina.

3.11. No se debe abrir ningún documento adjunto procedente de direcciones de correo desconocidas o no solicitados. Se recomienda que este tipo de e-mail sean eliminados en forma inmediata.

4. Antivirus

Objetivo: Evitar la contaminación por virus informático u otro código de software malicioso de programa.

4.1. Está prohibido a los empleados cargar software no autorizado a un computador o equipo de la red de PazCorp sin la autorización del área de TI.

4.2. Todo medio magnético de almacenamiento (DVD, CD, Disco duro externo, pendrive, o similar) debe ser examinado en busca de virus antes de introducirse a un computador de la red corporativa de PazCorp.

4.3. Todo correo electrónico que entre o salga (incluídos sus adjuntos) será examinado en busca de virus antes de ser distribuído o transmitido. Esto se aplicará de manera automática por medio del sistema de antivirus de la Empresa.

4.4. Los empleados de la empresa tienen la responsabilidad de informar de inmediato (correo, telefónicamente, etc.) cada incidente relacionado con un virus al personal de Tecnología a través de la Mesa de Ayuda.

5. Uso de Recursos Tecnológicos

Objetivo: Los recursos informáticos y computaciones de Paz Corp. se utilizarán exclusivamente con fines laborales. PazCorp se reserva el derecho de acceder y revisar cualquier equipo de su propiedad en forma asistida (in situ) o remota que esté conectado a la red corporativa, así como bloquear o eliminar las cuentas de usuarios sin previo aviso o comunicación formal.

5.1. Todo hardware y software utilizado por los empleados de la empresa es de propiedad de PazCorp y, como tal, puede en cualquier momento, sin aviso previo, ser examinado por personal de Tecnología.

5.2. Los sistemas computacionales de PazCorp. deben utilizarse sólo para actividades del negocio.

5.3. El usuario del equipo tiene prohibido trasladar o reubicar, bajo ninguna circunstancia, el equipo computacional que tiene asignado. Sólo el área de TI tiene autorización para realizar traslados de equipos, dentro o fuera del recinto laboral. Esta medida no aplica a equipos portátiles.

5.4. El funcionario será responsable del buen uso que se dé al computador que se le ha asignado para realizar sus labores.

Tecnología puede verificar (local o remotamente) el estado del computador en cualquier momento para asegurar el correcto uso y funcionamiento del equipo. Si Tecnología detecta algún daño o problema originado por responsabilidad del trabajador, ya sea uso indebido del equipo, negligencia o simple descuido u omisión del usuario, será de responsabilidad del usuario asumir el costo que implique la reparación del equipo, conforme prescribe el artículo 58 del Código del Trabajo.

6. Seguridad de Software

Objetivo: Asegurar que PazCorp cumpla con la normativa legal local y operacional del uso de software computacional.

6.1. Los funcionarios de la empresa utilizarán en los equipos de computación de PazCorp, sólo software computacional debidamente autorizado y licenciado.

6.2. Cada persona es responsable por el resguardo de la información almacenada localmente en su quipo PC (disco duro local). El área de TI es responsable únicamente y exclusivamente por la información almacenada en los servidores en la unidad de red "V:".

6.3. La Gerencia de Tecnología es responsable de actualizar los computadores periódicamente con las actualizaciones y "parches" de sistema operativo y aplicaciones que se liberan semanalmente. Por lo anterior no es labor ni responsabilidad del usuario mantener ni realizar las actualizaciones del sistema operativo.

6.4. Sólo el área de TI está autorizada para instalar programas computacionales, aunque estos sean gratuitos o trials.

6.5. El software de PazCorp, documentación u otra información interna no se puede comercializar, usar ni transferir a terceros, esto está prohibido por ley.

7. Seguridad del Personal

Objetivo: Minimizar los problemas de seguridad derivados de factores humanos.

7.1. Se le permite el acceso a las salas de servidores o salas de comunicaciones sólo a personal autorizado.

7.2. A los funcionarios de la empresa se les prohíbe discutir asuntos comerciales relacionados con los sistemas informáticos incluyendo software y hardware sensibles de la empresa en lugares públicos, incluso con compañeros de trabajo.

7.3. Cambios de configuración, cambios al sistema operativo, y actividades relacionadas deben ser realizados sólo por el personal de Tecnología, NO por los usuarios finales, esto está expresamente prohibido.

7.4. Los usuarios no deben poner a prueba o intentar burlar o deshabilitar las medidas de seguridad definidas por la empresa.

Los incidentes relacionados con accesos no autorizados a sistemas (hackear), el acierto de contraseñas o duplicación ilegal de software, u otros intentos por contrarrestar las medidas de seguridad pueden ser consideradas delito o ilegales, y se considerarán graves violaciones de la seguridad de tecnología por lo que podrían dar lugar a la presentación de demandas en los tribunales de justicia.

8. Seguridad del Hardware de Computadores

Objetivo: Proporcionar la protección física a los equipos computacionales de PazCorp y asegurar que la información cuente con un nivel adecuado de protección.

8.1. Los usuarios deben tomar las medidas necesarias para que el equipo asignado por PazCorp en su poder o bajo su control sea protegido contra el robo, el daño accidental o intencionado por parte de terceros.

8.2. Los usuarios de equipos portátiles no deben dejar sus equipos en lugares abiertos, vehículos o lugares públicos. Es obligación y responsabilidad del usuario dejar estos equipos asegurados mediante la cadena de seguridad proporcionada por el área de tecnología al momento de su entrega o cualquier otro dispositivo que cumpla con este fin. El no observar esta medida básica de seguridad y en el caso de extravío o robo del equipo, el usuario será responsable de reponer este activo a la compañía al valor comercial vigente del equipo de acuerdo las cotizaciones de los proveedores especialistas, o valor promedio de mercado en caso de que el equipo se

encuentre descontinuado. La reposición del valor se hará conforme prescribe el artículo 58 del Código del Trabajo.

8.3. No se permite comer o beber al trabajar con elementos o dispositivos computacionales.

9. Seguridad de Datos

Objetivo: Hacer que los datos y la información de PazCorp estén siempre disponibles, confiables e íntegros.

9.1. El personal no puede acceder a los sistemas de computación ni la información almacenada sin la autorización requerida, ni tampoco puede hacer modificaciones no autorizadas al contenido de algún sistema computaciones de PazCorp, incluida la eliminación o cambio de los datos.

9.2. El personal es responsable de la disponibilidad, integridad y confidencialidad de los datos de los clientes y de las empresas almacenados en sus equipos y en todos los medios transportables.

9.3. En caso de que, por error o casualidad, el empleado tenga acceso a información confidencial, esta debe ser borrada y eliminada de su computador. Queda estrictamente prohibido realizar copias o reenviar dicha información dentro o fuera de la empresa.

9.4. DVD, CD, discos duros, pendrive u otro medio similar con información de PazCorp o clientes deben ser tratados como información confidencial.

9.5. Cuando un funcionario deja la empresa, debe devolver todo el equipamiento asignado, equipo y componentes en perfectas condiciones de uso.

9.6. Cuando un empleado detecte una posible violación accidental o intencionada de la seguridad de la información, debe denunciar el hecho al área de TI, quien deberá investigar la situación y generar un informe.

10. Administración de Incidentes de Seguridad

Objetivo: Cualquier funcionario del área de tecnología que tome razón de un incidente o una debilidad de seguridad (incluidas fallas de sistemas, inhabilitación del servicio, errores a causa de datos del negocio imprecisos o incompletos, violación de confidencialidad) debe informarlo en forma inmediata al área de TI.

Un incidente de seguridad es cualquier evento que pueda o haya afectado a:

- La confidencialidad de la información (guardada electrónicamente) de la empresa.
- La integridad de los datos de la empresa.

- La disponibilidad de los sistemas de tecnología de la Empresa.

Los incidentes de seguridad pueden clasificarse como sigue:

- **Incidente de virus:** la presencia de uno o más archivo(s) contaminado(s) por cualquiera de una variedad de virus en un computador o servidor.

- **Ataque a Recursos/Red:** Un incidente que potencialmente podría entorpecer el tráfico de la red o los sistemas operacionales, o comprometer la confidencialidad, integridad o disponibilidad de cualquier elemento de la red corporativa.

- **Incidente Operacional:** Un incidente en la red nacional o en las operaciones computacionales originado por una falla de hardware o software, o un cambio legítimo hecho a un sistema por el personal operacional, que impide que los usuarios locales obtengan acceso.

11. Delitos Informáticos Ley 21.459

Objetivo: Proteger a Paz Corp y a sus colaboradores de verse expuestos y evitar la ocurrencia de situaciones que podrían dar origen o ser constitutivos de alguno de los delitos informáticos listados en la Ley 21.459. Además de velar por el cumplimiento de los principios de integridad, transparencia y honestidad que deben regir la conducta de los colaboradores de Paz Corp.

11.1. Esta estrictamente prohibido atacar la integridad de un sistema informático interno o externo, obstaculizar o impedir su normal funcionamiento (total o parcial).

11.2. Esta estrictamente prohibido acceder a un sistema informático interno o externo superando las barreras técnicas o medidas tecnológicas de seguridad, sin autorización o excediendo la autorización que se posea (Acceso Ilícito).

11.3. Esta estrictamente prohibido la interceptación ilícita de datos interna o externa.

11.4. Esta estrictamente prohibido atacar la integridad de los datos informáticos, ya sea, alterando o suprimiendo datos informáticos, causando un daño al titular de estos de forma indebida.

11.5. Esta estrictamente prohibido introducir, alterar, dañar, o suprimir datos informáticos (Falsificación Informática) con la intención de que sean tomados como auténticos o que sean utilizados para generar documentos auténticos de forma indebida.

11.6. Esta estrictamente prohibido comercializar, transferir o almacenar a cualquier título, datos informáticos cuyo origen sea ilícito y sean utilizados en interés o para provecho de la Empresa y/o sus entidades relacionadas.

11.7. Esta estrictamente prohibido manipular un sistema informático interno o externo, mediante la introducción, alteración, daño o supresión de datos informáticos, o a través de cualquier interferencia en el funcionamiento del sistema informático, causando, por una parte, un perjuicio, y por otra, un beneficio (Fraude Informático).

11.8. Esta estrictamente prohibido entregar, importar o difundir dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares para la perpetración de delitos informáticos (tales como el ataque a un sistema o a un dato informático, el acceso ilícito al mismo, o la interceptación ilícita).

El incurrir en cualquiera de las conductas antes descritas podrán ser consideradas como incumplimiento grave de las obligaciones del trabajador, pudiendo ser aplicadas las infracciones y medidas disciplinarias del sistema de prevención de delitos.