Política de Seguridad Informática

2015

I. OBJETIVO

El objetivo de este documento es proveer la información necesaria a los usuarios, empleados y gerentes, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la Red, así como la información que es procesada y almacenada en estos.

Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de Paz Corp. S.A. y sus filiales, en adelante "Paz".

II. ALCANCE

El contenido de este procedimiento aplica a todos los trabajadores de Paz.

III. RESPONSABILIDADES

Los responsables de su utilización y ejecución serán directamente los usuarios.

IV. DESCRIPCIÓN DEL PROCEDIMIENTO

1. Seguridad de la Red

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

1.1. Todo usuario de la red de Paz, debe ser autenticado mediante al menos un nombre de usuario (username) y una contraseña (password). Cada funcionario de Paz tiene estrictamente prohibido compartir o revelar su identificación personal o contraseña a otros y 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 Paz a un empleado deben ser cambiadas por éste la primera vez que se conecta. A su vez las contraseñas:

- Deben consistir en un mínimo de ocho caracteres de extensión y deben estar constituídas por caracteres alfanuméricos (números, letras y caracteres especiales)
- Deben ser cambiadas al menos cada dos meses.
- Deben ser cambiadas de inmediato si el usuario cree que la contraseña ha trascendido.
- Nunca deben escribirse en lugar visible.
- No deben reutilizarse una vez cambiadas. De acuerdo con las políticas de la empresa, el sistema guarda un histórico de 5 registros.

- Debe ser cambiada de inmediato si el usuario advierte actividad sospechosa o anormal en su computadora.
- Debe mantenerse en forma confidencial y nunca debe ser compartida o divulgada con los demás.

1.3. 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.

1.4. Está estrictamente prohibido el uso de equipos personales computacionales o de impresión para desempeñar labores profesionales dentro de la red de Paz. Paz 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 de Paz, por el riesgo de seguridad y confidencialidad de la información de Paz y la vulnerabilidad de esta política.

2. Uso de Internet

Objetivo: El personal de Paz debe utilizar internet exclusivamente como herramienta de trabajo asociada a sus labores sin exponer la seguridad de la información de ésta.

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

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

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

El área de Tecnología, en adelante "Tecnología", controlará y administrará los accesos a Internet mediante software especializado con el fin de asegurar el rendimiento y seguridad de la red computacional de Paz.

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

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

3. E-Mail

Objetivo: El personal debe utilizar el e-mail de Paz de manera eficaz y apropiada a sus funciones y labores.

3.1. Se prohíbe a los empleados usar el correo de Paz 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 Paz.

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 Paz.

3.3. Paz 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 el envío de material confidencial o información estratégica de Paz mediante el sistema de e-mail o correo.

3.5. Es de responsabilidad del empleado la revisión y limpieza periódica de su casilla de correo así como archivar localmente sus correos electrónicos a modo de respaldo.

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

3.7. Nunca se debe enviar por correo su nombre de usuario y/o contraseña, códigos de alarmas, combinación de caja fuerte o cualquier otra información que se utilice para dar acceso a oficinas, sistemas, bienes o servicios de Paz.

3.8. 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.

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

3.10. Los usuarios no podrán enviar correos electrónicos de más de 15 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 Paz.

3.11. 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 Paz al momento de la ausencia.

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 una computadora o equipo de la red de Paz sin la autorización del área de TI.

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

4.3. Todo e-mail 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 Paz.

4.4. Los empleados de Paz tienen la responsabilidad de informar de inmediato (por teléfono, por correo, 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 se utilizarán exclusivamente con fines laborales. Paz 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 Paz es de propiedad de ésta y, como tal, puede en cualquier momento, sin aviso previo, ser examinado por personal de Tecnología.

5.2. Los sistemas computacionales de Paz 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 Tecnología, tiene autorización para realizar traslados de equipos, dentro o fuera del recinto laboral.

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 de la computadora en cualquier momento para asegurar el correcto uso y funcionamiento del equipo. Si Tecnología detecta algún daño o problema originado por 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.

6. Seguridad de Software

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

6.1. Los funcionarios de Paz utilizarán en los equipos de computación de Paz, 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 Tecnología 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 Tecnología está autorizada para instalar programas computacionales, aunque estos sean gratuitos o trials.

6.5. El software de Paz, 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 Paz se les prohíbe discutir asuntos comerciales relacionados con los sistemas informáticos incluyendo software y hardware sensibles de Paz 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 Paz.

Los incidentes relacionados con accesos no autorizados a sistemas (hackear), el acierto de contraseñar 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 Paz 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 Paz 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 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 Paz 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.

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 Paz 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 computacional de Paz, 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, este debe ser borrada y eliminada de su computador. Queda estrictamente prohibido realizar copias o reenviar dicha información dentro o fuera de Paz.

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

9.5. Cuando se termina la relación contractual entre Paz y un funcionario, éste 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 a Tecnología, quien deberá investigar la situación y generar un informe.

10. Administración de Incidentes de Seguridad

Cualquier funcionario de Paz 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, entre otros) debe informarlo en forma inmediata a Tecnología.

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

- La confidencialidad de la información (guardada electrónicamente) de Paz.
- La integridad de los datos de Paz.
- La disponibilidad de los sistemas de tecnología de Paz.

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.

Elaboró	Revisó y Autorizó
César Sepúlveda Boris Staropolsky	Ariel Magendzo