POLÍTICA DE SEGURIDAD INFORMÁTICA FGRSOFT

Fabiana Núñez
Federico Carneiro
Federico Moreira
Rita González

Control de Cambios

Fecha	Versión Documento	Creador	Link Documento
23/10/2018	1.0	Fabiana Nuñez- Federico Moreira - Federico Carneiro - Rita González	

Índice de Contenidos

Introducción

La política de seguridad surge como una herramienta para orientar a la organización sobre la importancia y sensibilidad de la información respecto a los servicios de la organización. Mediante la política de seguridad se establecen canales de comunicación y acción en relación a recursos y servicios informáticos del tambo; el objetivo principal es describir qué se va a proteger, cómo y por qué.

La alta dirección será responsable de la seguridad de la información, siendo la encargada de la implementación de controles que aseguren los activos del Tambo. Será su responsabilidad asegurar que todo el personal conozca y cumpla las políticas de seguridad desde el primer momento que cualquier usuario tenga contacto con la organización.

La política de seguridad se basa en las normas vigentes para la seguridad y protección de datos , acceso a la información y protección de información personal[1]

[1] https://www.agesic.gub.uy/innovaportal/v/302/1/agesic/ley-n%C2%B0-18331-de-11-de-agosto-de-2008.html

Objetivos

Los objetivos de la presente Política de Seguridad de la información son:

- Proteger la información del negocio evitando cualquier pérdida de información que signifique un problema para la empresa.
- Asegurar diferentes controles internos con el fin de cumplir las pautas establecidas
- Capacitar a usuarios internos de la organización
- Implementar acciones que prevengan daños y otras que recuperen y corrijan los procesos establecidos.
- Generar cultura y conciencia de la responsabilidad de todos los usuarios pertenecientes al tambo, de reportar amenazas o violaciones de seguridad.
- Asegurar la operativa continua del tambo a pesar de algún inconveniente detectado

Seguridad Organizacional

Alcance

Dentro de este apartado se detallan aquellas medidas que refieren a la integridad y salud organizacional ; se definen responsabilidades de la Alta Dirección, de TI y de los usuarios restantes. Se detallan políticas sobre el control de activos, la seguridad de los usuarios y la respuesta a incidentes.

Organización y Responsabilidades

La política se aplicará a todos los usuarios de la organización.
Dentro de la organización existen distintos niveles de responsabilidades respecto a las políticas de seguridad.

Responsabilidades de la Alta Dirección

- Administrar la información, el personal y los activos fundamentales de la organización
- Revisar y aprobar las políticas de seguridad
- Hacer cumplir las sanciones por incumplimientos de las mismas

Responsabilidades del Equipo de TI

- Monitorear el cumplimiento de las políticas establecidas
- Informar de incumplimientos de políticas a la Alta Dirección
- Examinar los incidentes de Seguridad de la Información
- Mantener actualizados los equipos de la organización para mitigar los riesgos de virus en los mismos
- Fomentar la capacitación de los usuarios respecto a la seguridad de la información
- Brindar soporte ante problemas en las estaciones de trabajo ya sea en la planta como en otras secciones del Tambo.
- Definir políticas de contraseñas seguras
- Asegurar que los usuarios externos que usen la red sólo accedan a información acotada y en un ámbito controlado.
- Promover mejoras pertinentes a la seguridad de la información a la Alta Dirección
- Llevar un inventario de todos los activos de la organización a fin de mantenerlos actualizados y monitoreados.

Responsabilidad de los Usuarios

- Hacer uso responsable del correo electrónico
- Realizar respaldos de sus datos
- Informar de anormalidades detectadas en su equipo de trabajo
- Mantener a salvo las contraseñas utilizadas
- Utilizar contraseñas seguras
- No divulgar información confidencial sobre el negocio
- Informar de anomalías en el uso de los dispositivos de trabajo
- No utilizar las estaciones de trabajo con fines personales

- Cada usuario será responsable de las credenciales personales para ingresar al aplicativo. Las credenciales son únicas y no podrán ser transferidas o utilizadas por otros usuarios. Cualquier acción no autorizada con un usuario, hará responsable al titular del mismo.

Control de Activos

Con el fin de proteger los activos de la organización se establece el documento de políticas de seguridad informática.
Cada departamento tendrá un responsable de velar por los activos más críticos de su departamento ya sean dispositivos, medios de información, datos, etc.
Los activos más críticos deberán tener un tratamiento especial tanto en su preservación física como lógica y sólo podrán manipularse por personal autorizado para ello.

Seguridad de los usuarios

Capacitación a usuarios

Todo miembro de la organización recibirá una capacitación y concientización sobre la política de seguridad del Tambo. Aquellos miembros de la organización que desempeñen funciones vitales, vinculadas con la seguridad de la información recibirán apoyo y seguimiento tanto en la capacitación como en el manejo de herramientas que contribuyan a la correcta aplicación de las políticas de seguridad establecidas.
Todos los usuarios recibirán capacitación en el manejo de contraseñas seguras y protección de datos personales.

Reporte de Incidentes

Ante cualquier sospecha o certeza de pérdida o divulgación de datos del tambo a personas no autorizadas, se debe reportar de forma inmediata al departamento de seguridad de TI del tambo.
Deberán informarse también pérdidas o divulgación de contraseña .
Aquellos incidentes que involucren HW o problemas con el SW que amenacen la disponibilidad e integridad de la información, también deberán ser reportados.

Respuesta a incidentes

Frente a un reporte de incidente, el departamento de Sistemas deberá analizar el caso, diagnosticar, informar a Alta Dirección y disparar los planes de contingencia y recuperación Dependiendo de la naturaleza del incidente, se analizará la mejor estrategia de solución y respuesta al usuario informador.

Seguridad Lógica

Control de Acceso

Cada miembro de la organización será responsable del mecanismo de acceso que se le brinde, ya sea de tarjeta electrónica con RFID, usuario y password de acceso al aplicativo o cualquier otro sistema que contenga datos de la organización. Será responsable de no difundir sus credenciales ni utilizar credenciales que no sean suyas para ninguna tarea.

Mantenimiento de usuarios

De forma periódica deberán revisarse los permisos de cada política de usuarios con el fin de mantenerlos actualizados.
Ante una desvinculación de cualquier funcionario del tambo, se deberán dar de baja accesos a todos los sistemas a los que tenía acceso.

Se deberá llevar registro de todas las personas que visitan o acceden al tambo con su respectivos permisos dentro del mismo. Asimismo, deberá incorporarse un detalle diario de usuarios que acceden a la sala de servidores.

Internet

El personal de TI idóneo será el encargado de brindar servicio de internet a todos aquellos usuarios que presenten la necesidad de acceso de acuerdo a la función que desempeñen dentro del Tambo.
Los usuarios con acceso permitido a Internet no deberán navegar con fines personales ni descargar ningún tipo de SW no autorizado por el personal de TI.

Seguridad de Redes

El objetivo de este apartado es asegurar el acceso a internet de forma segura, dependiendo del sistema o activo al que se acceda.
Se consideran zonas inseguras a todas aquellas redes que no son controladas por el Departamento de TI.
TI asegura y administra un segmento de la red al que se denomina Zona Controlada,el cual acceden solo usuarios autorizados y se rigen por las políticas de seguridad correspondientes a su rol y perfil.
Cualquier visitante, socio, cliente ajeno al personal del tambo, podrá conectarse a la red configurada para ello, independiente del acceso del personal del tambo.
Solamente podrán conectarse por VPN a la LAN del tambo aquellos usuarios autorizados.
Todos los usuarios que establezcan conexión real con el tambo a través de Internet deberán utilizar mecanismos seguros y encriptados.
Todas las conexiones de la LAN y la DMZ hacia y desde Internet deberán pasar por un Firewall.

Software Malicioso

El departamento de TI será el encargado de proporcionar mecanismos de antivirus y protección en todos los dispositivos del establecimiento; sin embargo, todos los empleados serán responsables de no interrumpir el servicio de antivirus o cualquier actualización que estos requieran. Todos los sistemas o aplicaciones utilizadas en el establecimiento deberán ser analizadas por antivirus. Los empleados deberán analizar cualquier medio de almacenamiento externo que conecten a un dispositivo del establecimiento,siendo requisito fundamental para su uso.

Las actualizaciones de los sistemas de protección se realizará de forma centralizada a través de políticas de uso, y será responsabilidad del área de TI realizarlas de forma periódica y progresiva según la criticidad del servicio que se pueda ver afectado.

Cualquier miembro del tambo que reciba una alerta o amenaza de virus deberá desconectar su equipo de la red y avisar de forma inmediata al departamento de TI.

Políticas de Backup

Toda información o sistema relevante del establecimiento tendrá una política de respaldo periódica.

Cada sistema crítico será respaldado de forma tal de acceder a los mismos si fuera necesario y no afectar la operativa del tambo.

Todos los respaldos deberán almacenarse en un lugar seguro y protegido físicamente , en un lugar preferentemente independiente de la ubicación de los sistemas principales, de forma tal de evitar que ante una pérdida de un sistema principal, también se vea afectado su respaldo.

Seguridad Física

Contexto y protección de equipos

Dentro de las políticas de seguridad se definen mecanismos de seguridad física de todos los dispositivos que componen el Tambo.
Se deberán proteger dispositivos de escritorio, dispositivos móviles, servidores, base de datos
El acceso al predio del tambo será solo a miembros autorizados previamente.
Para servidores y equipos críticos se prevé un sistema de UPS con el fin de brindar disponibilidad de la información de forma ininterrumpida.
Se dispondrá de cámaras de seguridad para el monitoreo

Seguridad física y ambiental

- Se contemplan medidas de protección tales como instalación de detectores de humo y extintores tanto a nivel de planta como en otros departamentos
- Se contempla la instalación de pararrayos a nivel del predio.
- Se colocarán dispositivos alejados de ventanas
- El techo y piso de la sala de servidores tendrá un acondicionamiento especial de forma tal de controlar la humedad y estática del lugar. Esta sala además deberá contar con materiales resistentes al fuego y protegidas del polvo y calor.
- La sala de servidores contará con mecanismos especiales de enfriamiento con el fin de asegurar el correcto funcionamiento de los equipos que se encuentren en ella.
- Se deberá establecer un proceso de mantenimiento preventivo a antenas externas con el fin de asegurar las mismas teniendo especial atención en épocas de vientos fuertes.

Seguridad del perímetro

La conexión a internet se realizará según lo establezca el equipo de TI.
Se asegurará el perímetro a través de un Router de Acceso, encargado de bloquear cualquier conexión que no sea establecida por los protocolos de seguridad del equipo de TI .
Se establecerán diferentes zonas de acceso, todas deberán contar con Firewall con reglas específicas.

Control de acceso físico

El acceso físico al Tambo estará vigilado por personal específico.
Cualquier persona ajena al tambo que requiera acceder al área de servidores, deberá estar acompañado de personal del tambo responsable de asegurar la integridad de los mismos.
Se deberá llevar un registro de toda persona ajena a la organización que visite el establecimiento,indicando fecha, hora, motivo de la visita y permanencia, además de los datos personales de dicha persona.

La sala de servidores y toda aquella oficina donde se manejen datos sensibles de la organización, deberán tener acceso restringido mediante medios electrónicos. Se dispondrá de tarjetas con RFID en la que cada persona autorizada será responsable de portar y no compartir con miembros no autorizados.
El acceso mediante estos medios electrónicos guardará los datos de acceso con el fin de monitorear la entrada y salida de cada persona a los sitios mencionados.
El acceso físico en general del predio, como se indicó anteriormente, estará vigilado por personal capacitado, quien tendrá una lista de personal autorizado a ingresar al tambo y será notificado de aquellas personas que lo visiten con previa antelación. Toda persona no autorizada, no podrá ingresar al predio.

Mantenimiento de Equipos

Todos los dispositivos, sean de escritorio como laptops o dispositivos móviles utilizados en la planta deberán contar con un sistema operativo otorgado y acondicionado por el personal de TI. Los equipos deberán mantenerse actualizados tanto a nivel de sistema operativo como Firewall.

Se estipulan dos tipos de mantenimiento a los equipos: Mantenimiento lógico preventivo en el cual se mantendrán los discos de los equipos críticos en condiciones óptimas de procesamiento y Mantenimiento básico preventivo en el cual se asegurará una correcta limpieza de residuos, polvo o cualquier otra partícula que pueda afectar el uso correcto del equipo.

Incumplimiento de Políticas de Seguridad

Cualquier irregularidad o incumplimiento de la presente política puede devenir en acciones disciplinarias que podrán variar de acuerdo a la gravedad o impacto del riesgo o daño ocasionado.

La difusión de la política de seguridad es responsabilidad de la Alta Dirección y su acatamiento y apropiación por parte del personal deberá ser absoluta.

Pautas de revisión de política

Será fundamental que la política de seguridad continúe en el marco de un proceso de actualización adecuado al plan y contexto de la organización. Deberán ajustarse en caso de crecimiento del negocio, cambios a nivel de personal o de infraestructura, así como también nuevas tecnologías de desarrollo o incorporación de nuevos productos o servicios.