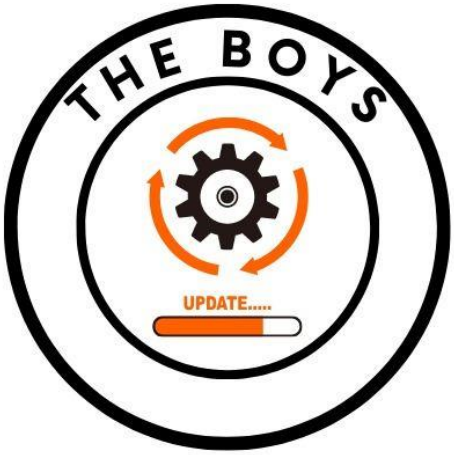

Políticas de Seguridad Informática (PSI)

PROYECTO FINAL

4o semestre Año 2022

INFORMACIÓN DEL DOCUMENTO

Nombre de Proyecto:	Proyecto Final	
Preparada por:	Diaz, Ariadna Lopez, Federico Torena, Nahuel Vazquez, Christofer Santana, Joaquín	**Fecha:** 20/ 11 / 2022

Versiones

Ver. No.	Fecha Ver.	Actualizado por:	Descripción
1.0	10/10/2022	The Boys	Sprint 3
1.1	05/11/2022	TheBoys	Sprint 4
1.2	20/11/2022	The Boys	Sprint 5

CONTENIDO

INTRODUCCION

Este documento se basa en las buenas prácticas que deben de tener los empleados para garantizar que los datos y la información delicada caiga en manos de terceros que puedan utilizarla a favor de sus propios intereses, se establecen los mecanismos necesarios para guardar y mantener la información segura y garantizar que esta esté disponible todo el tiempo para quienes estén autorizados a consultarla.

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 organización
- Implementar controles internos con el fin de cumplir las pautas establecidas.
- Capacitar a usuarios internos de la organización y brindar información a usuarios externos sobre las políticas y pautas de seguridad de la organización.
- Implementar acciones que prevengan daños
- Considerar aspectos de recuperación y corrección de mejora continua sobre los procesos establecidos.
- Generar cultura y conciencia de la responsabilidad de todos los usuarios de modo de generar reportes de amenazas o violaciones de seguridad de la información cuando corresponda.

ALCANCE

Dentro de este apartado se detallan aquellas medidas que refieren a la integridad y salud organizacional. 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 Gerencia General

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

Responsabilidades del Equipo de TI

- Generar inventario de activos de la organización y mantener dicha información actualizada y sistematizada.
- Actualizar equipamiento informático de cada usuario de modo de evitar riesgos de seguridad asociados a parches o vulnerabilidades de seguridad
- Monitorear el cumplimiento de las políticas establecidas
- Informar de incumplimientos de políticas a la Gerencia.
- Examinar los incidentes de Seguridad de la Información
- Proponer la cultura dentro de la organización con talleres, cursos y capacitaciones sobre aspectos de seguridad de la información
- Brindar soporte a usuarios tanto en equipos de escritorio, laptops y dispositivos móviles utilizados en campo.
- Definir políticas de contraseñas seguras que exijan cambio de forma periódica.
- Promover, asesorar y recomendar cambios e implementaciones de seguridad al equipo de Gerencia General.
- Asegurar que los usuarios externos que usen la red sólo accedan a información acotada y en un ámbito controlado.

ANALISIS DE RIESGOS

¿Qué datos se deben proteger?

Los bienes informáticos más importantes a proteger son:

- La red de interna LAN
- El servidor de aplicaciones.
- El Active Directory
- Los sistemas de Backup
- Las bases de datos de la aplicación web y mobile
- Las bases de datos de los dispositivos de la red

Las amenazas más importantes a considerar de acuerdo al impacto que pudieran tener sobre la infraestructura son:

- El acceso no autorizado a la red, tanto producto de un ataque externo como interno.
- Pérdida de disponibilidad.
- La sustracción, alteración o pérdida de información crítica.
- La introducción de programas que puedan vulnerar los sistemas críticos.
- El empleo inadecuado de las tecnologías y los servicios que estas ofrecen.

¿Dónde se encuentran?

Todos nuestros datos estarán registrados en la base de datos local Oracle, pero los usuarios pertenecientes al dominio serán registrados en la base de datos LDAP del Active Directory.

¿Qué procesos intercambian datos, entre qué entidades y estos intercambios se dan de forma segura?

Dentro de nuestra aplicación existen tres tipos de usuarios: Administradores, profesionales y comunes. Cada uno de ellos difiere en el tipo de información a la cual puede acceder, por ejemplo, un profesional no puede manipular los mismos datos que puede manipular un usuario administrador.

POLITICAS DE SEGURIDAD INFORMATICA

Autenticación de usuarios

En esta sección se explica el método de autenticación utilizado para comprobar la identificación de los usuarios ante los sistemas y aplicaciones existentes.

- Cómo son establecidas las contraseñas.
- Tipos de contraseñas utilizadas.
- Causas que motivan el cambio de contraseñas antes de que concluya el plazo establecido.
- Cuando se asigne inicialmente una contraseña temporal los usuarios deben ser forzados a cambiarla inmediatamente después del primer acceso.
- Las contraseñas serán únicas para cada persona y no deben ser descifrables.

Se exigirá a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas. Todos los usuarios deben de seguir estos pasos en cuanto a:

a) Mantener confidencialidad sobre la contraseña.

b) Evitar mantener un registro de contraseñas en texto claro en cualquier medio (por ejemplo, papel, archivo de software o dispositivo de mano).

c) Cambiar las contraseñas cuando haya una indicación de riesgo en el sistema o en la contraseña.

d) Seleccionar contraseñas de calidad con suficiente longitud mínima que sean:

1. Fáciles de recordar.

2. No se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento.

e) No incluir contraseñas en ningún proceso automatizado de conexión.

f) No compartir las contraseñas de usuario individuales.

g) No utilizar la misma contraseña para propósitos de trabajo y particulares.

REGLAMENTO INTERNO

- Deberán mantener limpio y en buen estado sus lugares de trabajo.
- El teléfono es para cuestiones de trabajo, por lo que se debe utilizar lo menos posible en asuntos personales.
- El equipo que utiliza cada empleado es responsabilidad suya, por lo que deberá cuidarlo y mantenerlo en buenas condiciones.
- No se debe Fumar, Comer o Beber dentro del área de trabajo.
- Solo personal autorizado puede entrar a las oficinas.
- Procurar no transportar información sensible en dispositivos extraíbles. En caso de hacerlo, encriptar la información.
- Utilizar solo las aplicaciones que están permitidas
- No instales aplicaciones no autorizadas en los equipos.
- Procurar no transportar información sensible en dispositivos extraíbles. En caso de hacerlo, encriptar la información.
- Acceder sólo a las páginas web confiables que se encuentran dentro de este documento o en las cuales aparezca «https» al inicio de la dirección web. De otro modo toda la información que ingrese podrá ser observada por terceros.
- Evitar guardar la información sensible en lugares físicos.
- No compartir ningún tipo de información de la organización con terceros.

- Actualizar los equipos con los que está trabajando siempre y cuando haya actualizaciones disponibles.

- No realice cambios en la configuración estándar de los sistemas sin autorización.

- Cierre la sesión del sistema o bloquéelo cuando se ausente de su computadora de (aunque sea de manera temporal).

- No revele información interna, principalmente de personas físicas, a terceros no identificados o que no estén debidamente autorizados.

- Evite tomar fotografías en ambientes laborales, sobre todo si piensa compartirlas en redes sociales o sistemas de mensajería instantánea, ya que pueden incluir vistas de pantallas, notas u otros papeles o sistemas que revelen información sensible.

- Evite usar dispositivos personales (teléfonos, tabletas, laptops) que no estén expresamente autorizados para almacenar o procesar datos laborales. Los dispositivos personales están más expuestos a robos, extravío y roturas, y tienen un riesgo mucho mayor de contener software malicioso, como virus, troyanos y spyware.

- Evite usar almacenamientos en Internet (como Dropbox o Drive) que no estén expresamente autorizados. La información almacenada en la «nube» está expuesta a ataques las 24 horas del día, y dificulta verificar con quién fue compartida y si el acceso de terceros fue retirado cuando ya no la necesitaban.

- No pulses en ningún enlace ni descargues ningún archivo adjunto de un mensaje de correo electrónico que presente cualquier indicio o patrón fuera de lo habitual. No confíes únicamente en el nombre del remitente. Comprueba que el dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual, contacta con ese contacto por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo

- Evita pulsar directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, es recomendable buscar información del mismo en motores de búsqueda como Google.

- No ejecutes nunca programas de origen dudoso o desconocido

Capacitación a usuarios

Todo miembro de la organización recibirá capacitaciones y talleres periódicos sobre políticas de seguridad y formas de preservar la información de la organización.
Toda persona que además desempeñe un rol vinculado directamente a la seguridad de la información deberá cumplir con al menos 100 horas de capacitaciones anuales que contribuirán a la correcta aplicación y uso de herramientas que aseguren el correcto funcionamiento y uso de las políticas establecidas.
Se brindarán además talleres y boletines periódicos sobre el uso y aplicación de buenas prácticas

Reporte de Incidentes

Ante cualquier sospecha o certeza de pérdida o divulgación de datos de cualquier índole perteneciente a la organización, ya sea de personas autorizadas o no autorizadas se debe reportar de forma inmediata al departamento de seguridad de TI.
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 Gerencia General y disparar los planes de contingencia y recuperación. Cada incidente se analizará de forma individual y se seleccionará la mejor forma de solución y respuesta.
En todo momento, el equipo de TI será responsable de mantener informado al resto de los usuarios afectados por el incidente detectado.

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.

Cualquier otro usuario ajeno a la organización que visite el predio podrá utilizar el servicio de internet a través de una red configurada para este tipo de usuarios
Todas las conexiones de la LAN 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 de la organización; así mismo, los usuarios finales también serán responsables no sólo del correcto funcionamiento de estos procesos sino también del reporte al equipo de TI si el mismo no funciona correctamente, generando un ticket para su correcto seguimiento y solución.

Utilizaremos un antivirus para uso corporativo que ayudará a proteger los sistemas, sus datos y los de los clientes, al tiempo que proporciona un control centralizado y escalabilidad para

una protección avanzada. El objetivo de un AV corporativo es proteger los dispositivos y hardware, correos electrónicos, entorno de nube, información IP y datos, entre otras áreas.

Por tal motivo optamos por el AV corporativo llamado Bitdefender este antivirus ofrece una protección continua y potente contra cualquier amenaza sofisticada.

Las características incluyen la función GravityZone, una seguridad de endpoints por capas adaptable diseñada para la nube y la virtualización, que protege a la empresa de ataques dirigidos avanzados a través de su arquitectura de supervisión e introspección de hipervisor, protección de endpoints por capas de próxima generación contra amenazas cibernéticas para detectar amenazas persistentes avanzadas y protección de su organización contra ataques de rescate y derrotas, y ataques de día cero.

También tiene el GravityZone Endpoint Security HD con HyperDetect con modelos de máquinas locales especializados y técnicas de análisis de comportamiento entrenadas para detectar y detectar herramientas de hacking, ofuscación de malware y exploits.

Para la infraestructura, este antivirus bloquea eficazmente los ataques que la mayoría de los endpoints tradicionales y las defensas antivirus de próxima generación no lo hacen.
Es responsabilidad de todos los usuarios, analizar y utilizar de forma segura cualquier medio de almacenamiento externo que conecten a un dispositivo.
Las actualizaciones de los sistemas de protección se realizarán de forma centralizada a través de políticas de uso, y será responsabilidad del equipo de TI. Dichos mantenimientos serán programados de forma paulatina, escalada y fuera de horario laboral.
Ante cualquier amenaza sobre un dispositivo, se deberá desconectar de forma inmediata de la red e informar al equipo de TI.

Estrategia de cumplimiento del PSI

Para verificar que los empleados y usuarios de la organización siguen las recomendaciones del documento PSI, se harán dos veces al año ataques controlados de ingeniería social con el motivo de chequear como actúan los usuarios ante un posible ataque de ese tipo para posteriormente obtener resultados de cuantos empleados fueron capaces de reconocer que estaban ante una situación sospechosa y cuantos empleados no fueron capaces de identificar que estaban ante un ataque informático.

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 Gerencia y su acatamiento y apropiación por parte del personal deberá ser absoluta.

.