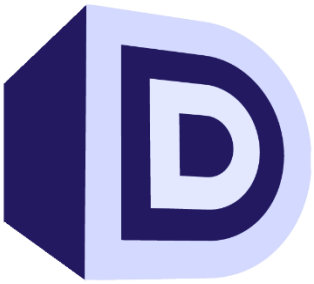

Digital Team

Políticas de Seguridad

22/05/2022

Versión **1.0**

Historial de revisiones

Autores:

Darien Miguel Sánchez Arévalo

Angel Alejandro Salinas García

Fernando De Luna Guardiola

Fecha	Versión	Descripción	Autor
22/05/2022	1.0	Elaboración Inicial del Documento	Darien Miguel Sánchez Arévalo

1. Introducción.

El presente documento tiene como objetivo ser una guía de apoyo para dar a conocer las reglas de seguridad que se tomarán con los recursos de la plataforma, en caso de que haya algún inconveniente y aclarar como actuaremos en estos casos. También veremos las distintas medidas de seguridad que implementamos.

1.1 Objetivo y ámbito de la aplicación.

El presente apartado del Documento de Seguridad para la Protección de Datos en Videojuegos y Privacidad tiene por objetivo establecer las directrices y actividades para la generación de cada uno de los elementos que conforman el Documento de Seguridad para la protección de los datos personales.

Considerando los siguientes artículos:

Artículo 6. Se refiere que la vida privada y los datos personales serán protegidos con las excepciones que fijen las leyes correspondientes.

Artículo 16. Señala que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición al uso de su información personal, en los términos que dije la ley, la cual establecerá los supuestos de excepción de principios de orden público, seguridad y salud pública o para proteger los derechos de terceros.

Artículo 33. Se establecen las actividades interrelacionadas que deben realizar los responsables para establecer y mantener las medidas de seguridad para la protección de los datos personales.

2. Glosario.

Documento de Seguridad. Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Datos personales. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Seguridad Perimetral. Un perímetro de red es el límite seguro entre el lado privado y administrado localmente de una red, a menudo la intranet de una empresa, y el lado público de una red, a menudo Internet.

Firewall. En informática, un cortafuegos es la parte de un sistema o una red informáticos que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

IPS. Un sistema de prevención de intrusos es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

IDS. Un sistema de detección de intrusiones es un programa de detección de accesos no autorizados a un computador o a una red.

Microsoft Azure. Microsoft Azure es un servicio de computación en la nube creado por Microsoft para construir, probar, desplegar y administrar aplicaciones y servicios mediante el uso de sus centros de datos.

Microsoft. La empresa desarrolla, fabrica, licencia y da soporte a ordenadores personales, servidores, dispositivos electrónicos y servicios.

Azure Firewall. Azure Firewall es un servicio de seguridad de firewall de red inteligente y nativo de la nube que le proporciona la mejor protección contra amenazas para las cargas de trabajo en la nube que se ejecutan en Azure.

DRP. Un plan de recuperación ante desastres es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

Bases de Datos. Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Nube. Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

BCP. Un plan de continuidad del negocio es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

3. Seguridad Perimetral.

Los puntos más importantes que conforman la seguridad perimetral tienen que ver con el **Firewall**, **IPS** (sistema de prevención de intrusiones) e **IDS** (sistema de detección de intrusos).

Dado que nosotros estamos utilizando los servicios de **Microsoft Azure** para alojar las máquinas virtuales: Al establecer las defensas de la nube de Azure, primero debe comprender que un sistema de detección de intrusiones (IDS, Intrusion Detection System) en Azure es fundamentalmente diferente que en entornos locales.

En Azure, no se administra la infraestructura de red subyacente, lo que dificulta el acceso a la información a nivel de paquete mediante la creación de reflejo de puertos, las pulsaciones o los métodos tradicionales basados en la red. **Microsoft** es responsable de proteger su infraestructura, ya que operan bajo el modelo de responsabilidad compartida. Sin embargo, usted sigue siendo responsable de supervisar y proteger las aplicaciones que se ejecutan en Azure.

Pero la manera que tenemos para manejar el IPS e IDS en Microsoft Azure es mediante el Firewall que nos proporciona el mismo servicio. Dado que **Azure Firewall** ofrece IPS/IDS.

4. DRP (Plan de Recuperación de Desastres)

4.1 Análisis de riesgos

Los datos personales a los que los servidores públicos tienen acceso en el ejercicio de sus atribuciones se resguardan de manera física y electrónica, según las necesidades de la actividad para la cual se lleva a cabo su tratamiento.

Tanto para la protección de datos personales, como para los datos sensibles, que son determinados junto con su ciclo de vida por las Unidades Administrativas, sin ser discriminados por su valor o ciclo de vida, pues su vulnerabilidad podría traer la divulgación o incluso un daño moral o patrimonial para los titulares de los datos, por lo tanto, el valor de los datos personales en la actualidad cobra cada día mayor relevancia por las implicaciones e información vinculados a ellos.

En este sentido, tanto los sistemas electrónicos como los medios a través de los cuales se resguardan de manera física los datos personales presentan diferentes particularidades debido a las características de cada uno de ellos.

Los datos personales que se guardan de forma física tienen diferentes tipos de riesgos existentes, los riesgos existentes son la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción; por ello, se cuenta con un área de soporte encargada de ejecutare acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y con acreditación para su uso.

Por su parte, los datos personales contenidos en un sistema electrónico presentan riesgos por su propia naturaleza como los son el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas, por ello, se cuenta con un área de soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos y previa acreditación de su personalidad a través de medios electrónicos para su uso.

4.2 Análisis de brecha

Las medidas de seguridad existentes y efectivas para la protección de datos personales con las que actualmente se cuenta son:

- **Medidas de seguridad:** La información que contiene datos personales se resguarda en una ubicación que cuenta con diversas medidas de seguridad como cámaras de seguridad, archiveros específicos para su resguardo y uso de cerraduras para su acceso.

- **Medidas de control:** Medidas de carácter administrativo encaminadas a contar con un registro físico de los servidores públicos que tienen acceso a datos personales, así como de los datos personales contenidos en los documentos.

- **Medidas legales**: Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos, se realiza el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.

- **Medidas cibernéticas:** Contamos con atribuciones para establecer normas y lineamientos e implementar esquemas de seguridad para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras.

5. BCP (Plan de Continuidad Empresarial)

5.1 Ámbito y objetivos.

Indica la finalidad del BCP, incluidas las funciones empresariales específicas a las que debe darse prioridad para garantizar la recuperación durante una emergencia.

Este **BCP** se usa para garantizar la continuidad de los servicios de **TI** y las líneas de clientes en el caso de una *interrupción* del suministro eléctrico imprevista y prolongada. La *interrupción* del suministro eléctrico podría estar causada por condiciones meteorológicas de emergencia o el incendio en un edificio. Las áreas funcionales que se priorizan para la recuperación en este BCP son el departamento de atención al cliente y el equipo de finanzas.

5.2 Operaciones en riesgo.

Incluye posibles riesgos con funciones operativas clave que interrumpirían en gran medida el negocio y la continuidad de los clientes.

Operación: Atención al cliente.

Descripción de la operación: el equipo de atención al cliente intenta, después de 24 horas, poner en marcha operaciones globales de chat en directo y llamadas de clientes.

Descripción del impacto: todos los chats en directo se realizan a través del equipo de atención al cliente de Digital Team. El 20 % de las llamadas en directo se dirigen a la oficina de Digital Team. Una interrupción quiere decir que ya no se podrán ofrecer servicios de asistencia mediante chat en directo y que los clientes experimentarán tiempos de espera prolongados en las llamadas, los plazos de los proyectos y los horarios del equipo.

5.3 Estrategia de recuperación

Describe todos los procedimientos relevantes para restablecer las operaciones empresariales después de un incidente o una crisis.

El personal de TI y los comités de BCP deben poner en marcha servidores y programas de reserva alternativos para guardar solicitudes de clientes después de una interrupción del suministro eléctrico. El servicio de atención al cliente debe ser capaz de recibir las solicitudes y responder a los clientes en un plazo de 30 minutos.

5.4 Funciones y responsabilidades

Hace referencia al personal clave y sus tareas asignadas durante o después de un incidente.

Representante: Darien Sánchez
Función: director de operaciones
Datos de contacto: darienmsa@example.com
Descripción de las responsabilidades:
1. Debe garantizar que los BCP se actualicen y debe coordinar los cambios con los responsables de equipo.
2. Ayuda a notificar a las principales partes interesadas en la región de EMEA sobre amenazas en las herramientas y los programas de atención al cliente.