



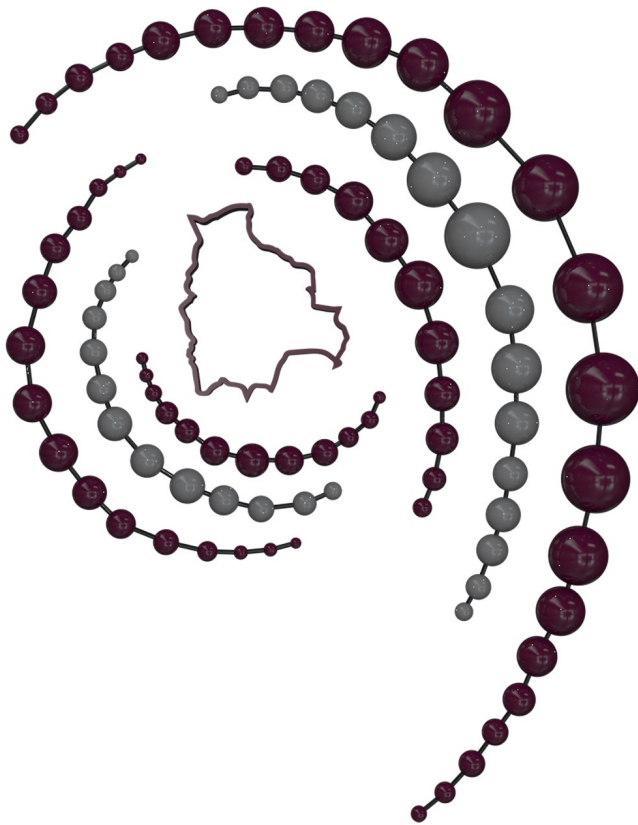
ESTADO PLURINACIONAL DE  
**BOLIVIA**

MINISTERIO DE  
LA PRESIDENCIA



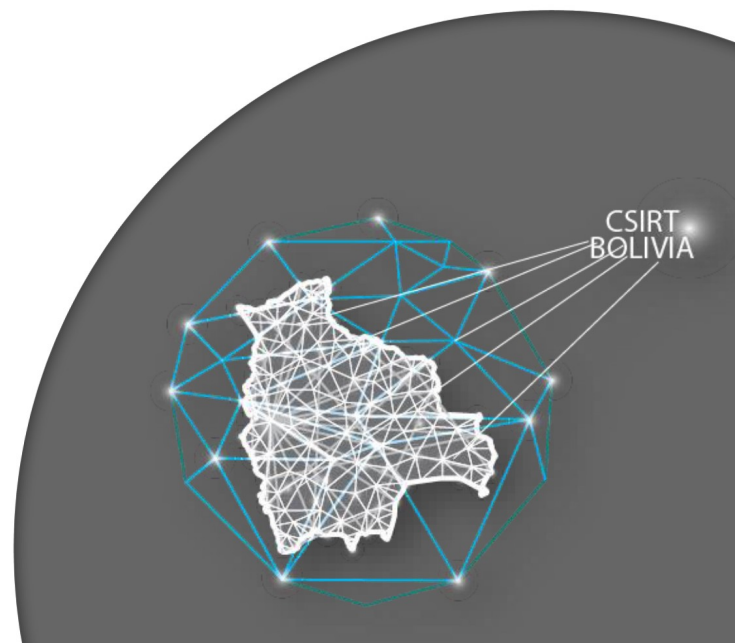
**AGETIC**  
Digitalizando Bolivia

Agencia de Gobierno Electrónico y  
Tecnologías de Información y Comunicación



# INFORME DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES INFORMÁTICAS

**GESTIÓN  
2021**



## Índice

|  |    |
|--|----|
| 1. Resumen Ejecutivo.....                                | 3  |
| 2. Alcances.....   | 4  |
| 3. Actividades.....                                      | 4  |
| 4. Estadísticas.....                                     | 5  |
| 4.1. Casos abiertos.....                                 | 5  |
| 4.2. Casos abiertos por categoría.....                   | 7  |
| 4.2.1 Incidentes.....                                    | 7  |
| 4.2.2 Vulnerabilidades.....                              | 8  |
| 4.3. Casos resueltos.....                                | 10 |
| 4.4. Casos resueltos por vulnerabilidad e incidente..... | 11 |
| 5. Términos y definiciones.....                          | 12 |
| 6. Historial de cambios.....                             | 15 |

## Índice de tablas

|  |    |
|--|----|
| Tabla 1: Detalle de casos abiertos.....                      | 6  |
| Tabla 2: Incidentes por categoría.....                       | 7  |
| Tabla 3: Vulnerabilidades por categoría.....                 | 8  |
| Tabla 4: Casos abiertos y resueltos.....                     | 10 |
| Tabla 5: Casos resueltos por vulnerabilidad e incidente..... | 11 |

## Índice de gráficos

|  |    |
|--|----|
| Gráfico 1: Casos abiertos.....                 | 6  |
| Gráfico 2: Incidentes por categoría.....       | 8  |
| Gráfico 3: Vulnerabilidades por categoría..... | 9  |
| Gráfico 4: Porcentaje de casos resueltos.....  | 10 |
| Gráfico 5: Tickets resueltos.....              | 11 |

## 1. Resumen Ejecutivo

El Centro de Gestión de Incidentes Informáticos (CGII) de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) publica el informe de gestión de incidentes y vulnerabilidades correspondiente a la gestión 2021, en el marco del Decreto Supremo 2514 que establece las funciones del CGII:

- Monitorear los sitios web gubernamentales y la aplicación de las políticas y lineamientos definidos por la AGETIC.
- Comunicar y otorgar información a todas las entidades del sector público acerca de incidentes informáticos y vulnerabilidades de los que se haya tomado conocimiento.
- Prestar soporte técnico a las entidades del sector público, en caso de que ocurriera un incidente informático.
- Otorgar soporte técnico para la prevención de incidentes informáticos a las entidades del Nivel Central del Estado a solicitud de las mismas.
- Coordinar la gestión de incidentes informáticos gubernamentales con entidades de similar función a nivel internacional.

Durante el año 2021, se gestionaron 367 casos de incidentes y vulnerabilidades informáticas, que corresponden a reportes nuevos y abiertos de meses anteriores. Del total de casos, 297 fueron resueltos a través de una correcta comunicación, seguimiento y validación con las entidades afectadas y 70 se encuentran abiertos, los cuales están siendo gestionados para su solución; los resultados serán reflejados en el presente informe.

El actual informe muestra estadísticas de la atención de casos válidos de incidentes y vulnerabilidades informáticas durante la gestión 2021, cuyos datos son clasificados por casos “tipo” en términos de cantidad y porcentaje.

También se hace una relación porcentual entre los casos que fueron resueltos en el transcurso del mes y aquellos que están en proceso de solución.

## 2. Alcances

La información de cantidades y porcentajes mostrados en el presente informe corresponde a casos gestionados por el CGII en la gestión 2021, a partir de los casos válidos de incidentes y vulnerabilidades informáticas originados por las siguientes fuentes:

- Responsables de Seguridad de la Información de las entidades del sector público.
- Herramientas de monitoreo y detección implementadas por el CGII.
- Equipos de Respuesta ante Incidentes Informáticos.
- Participantes del muro de la fama a través del formulario de reporte.

## 3. Actividades

A continuación las actividades realizadas por el CGII durante el referido período de tiempo:

- Análisis de indicadores de compromiso, obtenidos de fuentes abiertas de información que tuvieron incidencia en entidades del sector público.
- Validación de reportes para descartar falsos positivos que no corresponden.



- Comunicación de incidentes y vulnerabilidades informáticas a las entidades afectadas, brindando la información técnica necesaria para su solución.
- Seguimiento al estado de solución de los casos pendientes, a través de llamadas telefónicas y correo electrónico, así como soporte técnico, en caso de que así lo requieran.
- Validación de las medidas aplicadas por las entidades para solucionar el incidente o vulnerabilidad informática, y posterior cierre del caso.
- Monitoreo de disponibilidad de 548 sitios web pertenecientes a entidades del sector público.
- Detección de incidentes y vulnerabilidades informáticas realizadas a través del monitoreo continuo de sitios web gubernamentales.

## 4. Estadísticas

Las siguientes estadísticas presentadas en tablas y gráficos corresponden a casos abiertos y resueltos de reportes de incidentes y vulnerabilidades informáticas gestionadas durante el año 2021.

### 4.1. Casos abiertos

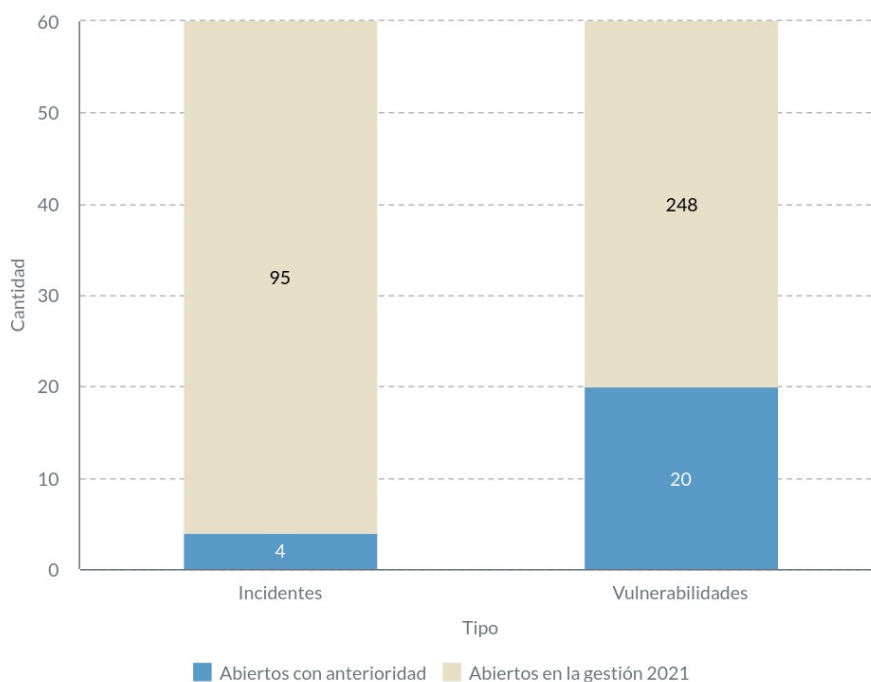
En este período, se gestionaron 367 casos de incidentes y vulnerabilidades informáticas, de los cuales, 343 fueron abiertos en la gestión 2021 y 24 corresponden a gestiones anteriores; en la siguiente tabla se podrá apreciar la información desagregada:

*Tabla 1: Detalle de casos abiertos*

| Tipo             | Descripción                 | Cantidad   |
|------------------|-----------------------------|------------|
| Incidentes       | Abiertos en la gestión 2021 | 95         |
|                  | Abiertos con anterioridad   | 4          |
| Vulnerabilidades | Abiertas en la gestión 2021 | 248        |
|                  | Abiertas con anterioridad   | 20         |
| <b>Totales</b>   |                             | <b>367</b> |

En el siguiente gráfico se puede observar la distribución de incidentes y vulnerabilidades informáticas abiertas en la gestión 2021 y con anterioridad:

*Gráfico 1: Casos abiertos*



## 4.2. Casos abiertos por categoría

### 4.2.1 Incidentes

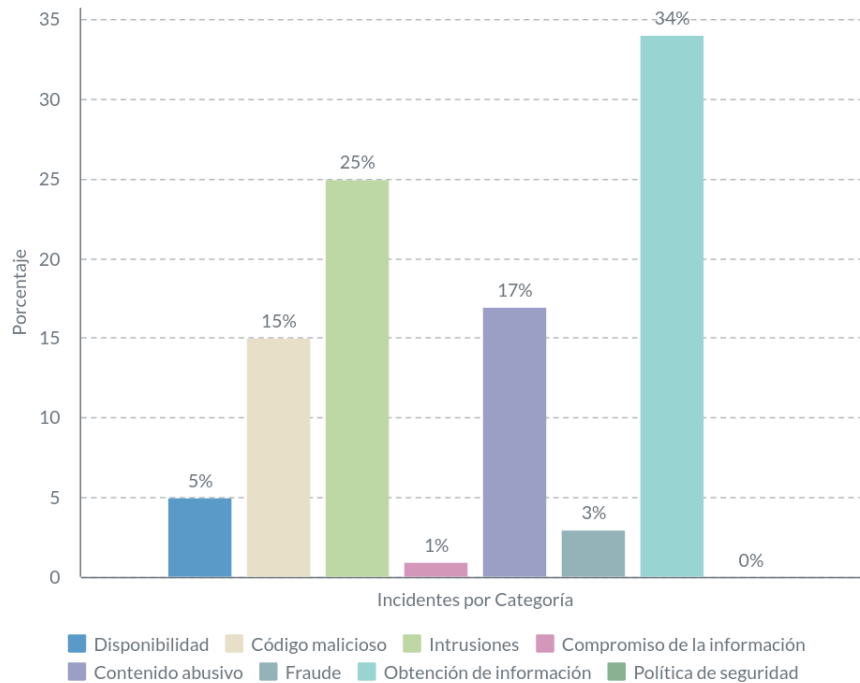
En la gestión 2021 se registraron 95 nuevos incidentes informáticos, que fueron categorizados de acuerdo al detalle, representado por la siguiente tabla y su respectivo gráfico:

*Tabla 2: Incidentes por categoría*

| Categoría                    | Cantidad  | Porcentaje   |
|------------------------------|-----------|--------------|
| Disponibilidad               | 5         | 5 %          |
| Código malicioso             | 14        | 15 %         |
| Intrusiones                  | 24        | 25 %         |
| Compromiso de la información | 1         | 1 %          |
| Contenido abusivo            | 16        | 17 %         |
| Fraude                       | 3         | 3 %          |
| Obtención de información     | 32        | 34 %         |
| Política de seguridad        | 0         | 0 %          |
| <b>Totales</b>               | <b>95</b> | <b>100 %</b> |

Dentro de las categorías: **obtención de información** e **intrusiones**, que cuentan con la mayor cantidad de incidencias, se gestionaron casos de spam, distribuidos a través de correos electrónicos con la finalidad de obtener la contraseña de los usuarios, e intrusiones a sitios web que provocaron modificaciones no autorizadas a los mismos.

Gráfico 2: Incidentes por categoría



#### 4.2.2 Vulnerabilidades

En la gestión 2021 se registraron 248 nuevos casos de vulnerabilidades, que han sido categorizados de acuerdo al detalle de la siguiente tabla y su gráfico:

Tabla 3: Vulnerabilidades por categoría

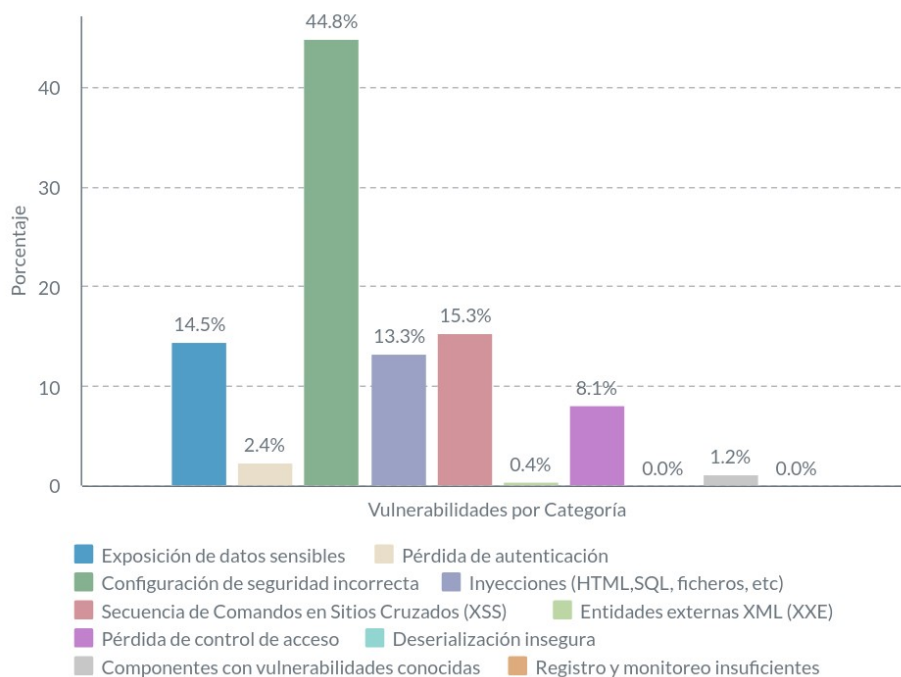
| Categoría                             | Cantidad | Porcentaje |
|---------------------------------------|----------|------------|
| Exposición de datos sensibles         | 36       | 14.5 %     |
| Pérdida de autenticación              | 6        | 2.4 %      |
| Configuración de seguridad incorrecta | 111      | 44.8 %     |
| Inyecciones (HTML, SQL, ficheros)     | 33       | 13.3 %     |



| Categoría                                      | Cantidad   | Porcentaje  |
|--|------------|-------------|
| Secuencia de Comandos en Sitios Cruzados (XSS) | 38         | 15.3 %      |
| Entidades externas XML (XXE)                   | 1          | 0.4 %       |
| Pérdida de control de acceso                   | 20         | 8.1 %       |
| Deserialización insegura                       | 0          | 0.0 %       |
| Componentes con vulnerabilidades conocidas     | 3          | 1.2 %       |
| Registro y monitoreo insuficientes             | 0          | 0.0 %       |
| <b>Totales</b>                                 | <b>248</b> | <b>100%</b> |

Como se aprecia en el gráfico, la detección de **Secuencia de Comandos en Sitios Cruzados (XSS)** y **Configuración de seguridad incorrecta**, predominaron durante la gestión 2021, presentes en sistemas de información de las entidades del sector público.

Gráfico 3: Vulnerabilidades por categoría



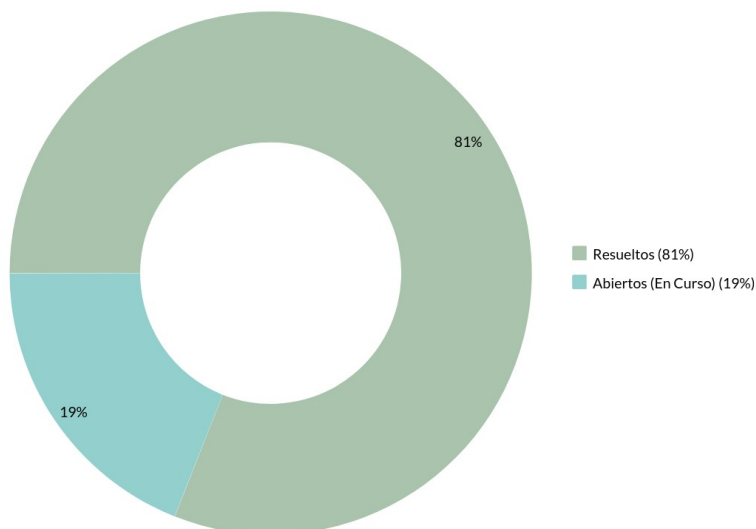
### 4.3. Casos resueltos

Como resultado de las actividades de gestión de incidentes y vulnerabilidades informáticas en la gestión 2021, el CGII resolvió 297 casos, quedando pendientes de solución para siguientes periodos 70 casos, a los cuales se está dando el seguimiento respectivo. Estos datos se aprecian en la siguiente tabla y su correspondiente gráfico:

*Tabla 4: Casos abiertos y resueltos*

| Estado              | Cantidad   | Porcentaje  |
|---------------------|------------|-------------|
| Resueltos           | 297        | 81 %        |
| Abiertos (En curso) | 70         | 19 %        |
| <b>Totales</b>      | <b>367</b> | <b>100%</b> |

*Gráfico 4: Porcentaje de casos resueltos*



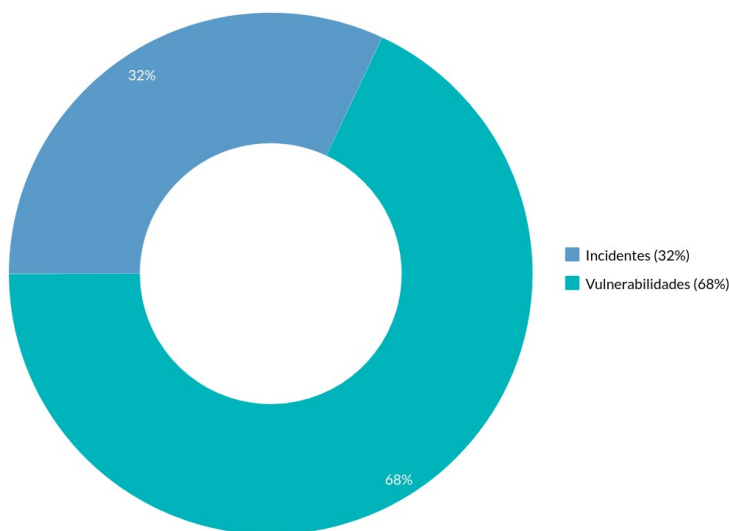
#### 4.4. Casos resueltos por vulnerabilidad e incidente

Del total de casos resueltos en la gestión 2021, 94 corresponden a incidentes y 203 a vulnerabilidades informáticas, datos que se pueden observar en la siguiente tabla y su correspondiente gráfico:

*Tabla 5: Casos resueltos por vulnerabilidad e incidente*

| Tipo             | Cantidad   | Porcentaje  |
|------------------|------------|-------------|
| Incidentes       | 94         | 32 %        |
| Vulnerabilidades | 203        | 68 %        |
| <b>Totales</b>   | <b>297</b> | <b>100%</b> |

*Gráfico 5: Tickets resueltos*



## 5. Términos y definiciones

**Código malicioso.-** Programas informáticos que tienen como objetivo acceder al sistema sin ser detectados y realizar acciones como el secuestro de información o recopilación de datos privados.

**Componentes con vulnerabilidades conocidas.-** Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación; si se explota un componente vulnerable, el ataque puede provocar pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas que pueden debilitar las defensas y permitir diversos ataques e impactos.

**Compromiso de la información.-** Acceso, modificación, borrado o publicación de información sin autorización del propietario.

**Configuración de seguridad incorrecta.-** Una configuración errónea de seguridad surge cuando dichas configuraciones se definen, implementan y se mantienen con valores predeterminados.

**Contenido abusivo.-** Incidentes que muestren signos evidentes de correos electrónicos no solicitados (spam).

**Deserialización insegura.-** Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos que pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

**Disponibilidad.-** Falta de disponibilidad del sistema o servicio producto de ataques de denegación de servicio, mala configuración, interrupciones de servicio por factores no previstos.

**Entidades externas XML (XXE).-** Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Un ataque de entidad externa XML exitoso puede revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).

**Exposición de datos sensibles.-** Acceso a datos sensibles como contraseñas, claves privadas de API, errores o debug, rutas completas, datos personales o uso de algoritmos de cifrado débil.

**Fraude.-** Incidentes que tengan nexo con el uso no autorizado, derechos de autor, suplantación de identidad, exfiltración de información o uso ilegítimo de credenciales.

**Incidente.-** Evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Intrusiones.-** Acceso al sistema o a uno de sus componentes aprovechando sus vulnerabilidades.

**Inyecciones.-** Son fallas de inyección, como SQL, NoSQL, OS o LDAP que ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta.

**Obtención de información.-** Obtención de datos personales, información de las redes de datos, credenciales de acceso del usuario a través de técnicas de engaño.

**Pérdida de Autenticación.-** Este tipo de debilidad puede permitir a un atacante capturar u omitir los métodos de autenticación que usa una aplicación web.

**Pérdida de control de acceso.-** Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos.

**Política de seguridad.-** Incidentes de abuso de privilegios de los usuarios, acceso a servicios no autorizados, o relacionados al uso de sistemas desactualizados.

**Registro y monitoreo insuficientes.-** El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permite a los atacantes mantener el ataque en el tiempo, pivotar a otros sistemas y manipular, extraer o destruir datos. Historial de cambios

**Secuencia de Comandos en Sitios Cruzados (XSS).-** Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador.

**Phishing .-** Conjunto de técnicas que consiste en engañar al usuario para robarle información confidencial.

**Caso abierto.-** Reporte de un incidente o vulnerabilidad informática que fue validado y se encuentra en proceso de solución.

**Caso resuelto.-** Reporte de un incidente o vulnerabilidad informática que fue resuelta satisfactoriamente.

**Vulnerabilidad.-** Debilidad o falla en un sistema de información que pone en riesgo la seguridad del mismo, permitiendo que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad.

## 6. Historial de cambios

| Versión | Fecha      | Autor             | Descripción | Motivo de cambios                   |
|---------|------------|-------------------|-------------|-------------------------------------|
| 1.0     | 10/01/2022 | Rodrigo Uruchi    | Elaboración | Datos iniciales, estructura y datos |
| 1.0     | 12/01/2021 | Jazmín Valdivieso | Revisión    | Redacción                           |
| 1.0     | 12/01/2021 | Franz Rojas       | Aprobación  | Aprobación                          |

