



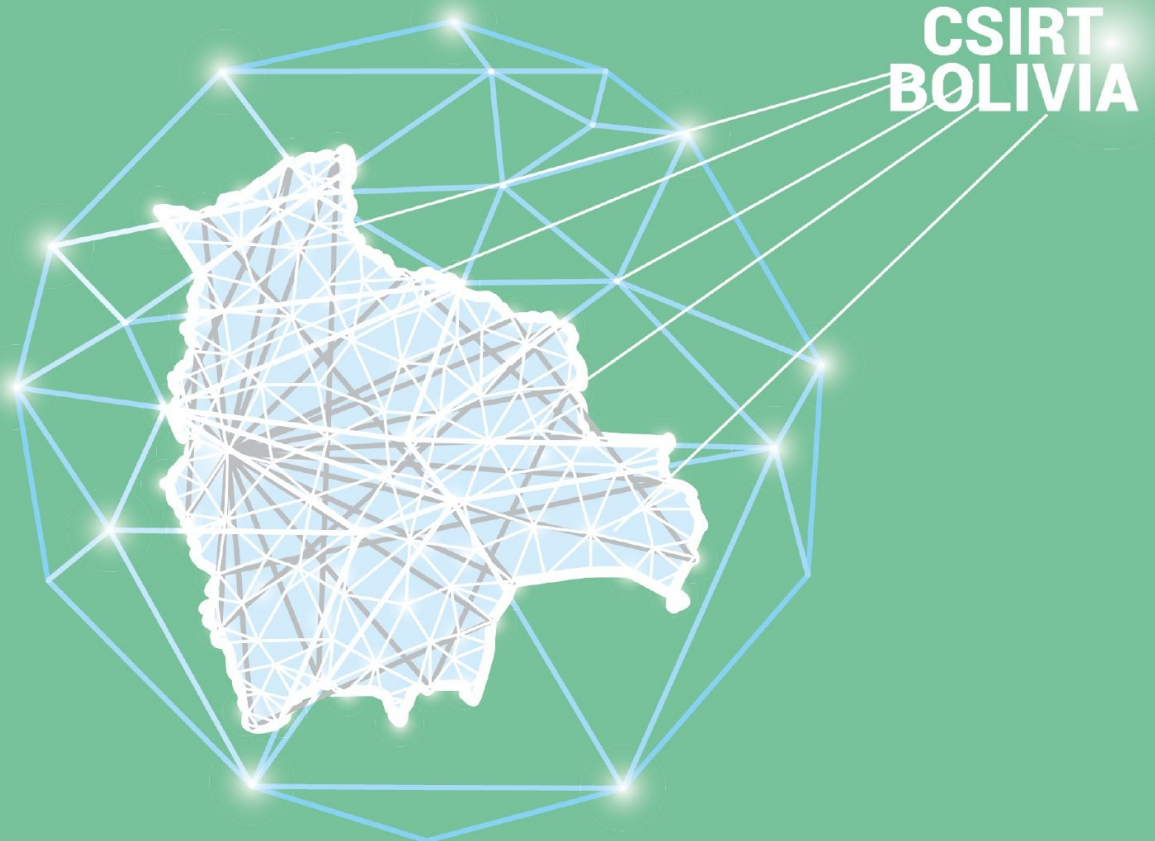
Gobierno del Estado Plurinacional de  
**BOLIVIA**  
Ministerio de la Presidencia



**AGETIC**  
agencia de gobierno electrónico y  
tecnologías de información y comunicación

# INFORME DE GESTIÓN DE INCIDENTES Y VULNERABILIDADES

OCTUBRE 2020





## Índice

1. Resumen Ejecutivo.....	3
2. Alcances.....	4
3. Actividades.....	4
4. Estadísticas.....	5
4.1. Tickets abiertos.....	5
4.2. Tickets abiertos por categoría.....	6
4.2.1 Incidentes.....	6
4.2.2 Vulnerabilidades.....	8
4.3. Tickets resueltos.....	9
4.4. Tickets resueltos por vulnerabilidad e incidente.....	10
5. Términos y definiciones.....	12
6. Historial de cambios.....	15

## Índice de tablas

Tabla 1: Detalle de tickets abiertos.....	5
Tabla 2: Tickets de incidentes por categoría.....	7
Tabla 3: Tickets de vulnerabilidades por categoría.....	8
Tabla 4: Tickets abiertos y resueltos.....	10
Tabla 5: Tickets resueltos por vulnerabilidad e incidente.....	11

## Índice de gráficos

Gráfico 1: Tickets abiertos.....	6
Gráfico 2: Tickets de incidentes por categoría.....	7
Gráfico 3: Tickets de vulnerabilidades por categoría.....	9
Gráfico 4: Porcentaje de tickets 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) presenta el informe de gestión de incidentes y vulnerabilidades correspondiente a octubre de 2020 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 que haya tomado conocimiento.
- Prestar soporte técnico a las entidades del sector público en caso de que ocurriese 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 este mes se gestionaron 128 tickets de incidentes y vulnerabilidades que corresponden a reportes nuevos y abiertos en meses anteriores. Del total de tickets, 89, fueron resueltos a través de la correcta comunicación, seguimiento y validación con las entidades afectadas; 39 tickets se encuentran abiertos y están siendo gestionados para solucionarlos, cuyos resultados están reflejados en el siguiente informe.

El presente informe muestra estadísticas de la atención de tickets válidos de incidentes y vulnerabilidades durante el mes de octubre, cuyos datos son clasificados por tipo en términos de cantidad y porcentaje.

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

## 2. Alcances

La información de cantidades y porcentajes mostrados en el presente informe corresponden a tickets gestionados por el CGII en octubre, a partir de reportes válidos de incidentes y vulnerabilidades realizadas por las siguientes fuentes:

- Responsables de Seguridad de la Información de las entidades del sector público.
- Herramientas de monitoreo y detección implementados 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 tienen incidencia en entidades del sector público.
- Validación de reportes para descartar falsos positivos que no corresponden ser atendidos.
- Creación de tickets para comunicar el incidente o vulnerabilidad a la entidad afectada, brindando la información técnica necesaria para su solución.
- Seguimiento al estado de solución de los casos pendientes a través de llamadas telefónicas y/o correo electrónico, otorgando soporte técnico en caso que así se requiera.

- Validación de las medidas aplicadas por la entidad para solucionar el incidente o vulnerabilidad, y posterior cierre del ticket.
- Monitoreo de disponibilidad de 551 sitios web pertenecientes a entidades del sector público.
- Detección de incidentes y vulnerabilidades.

## 4. Estadísticas

Las siguientes estadísticas presentadas en tablas y gráficos corresponden a tickets abiertos y resueltos de reportes de incidentes y vulnerabilidades gestionadas durante el mes de octubre.

### 4.1. Tickets abiertos

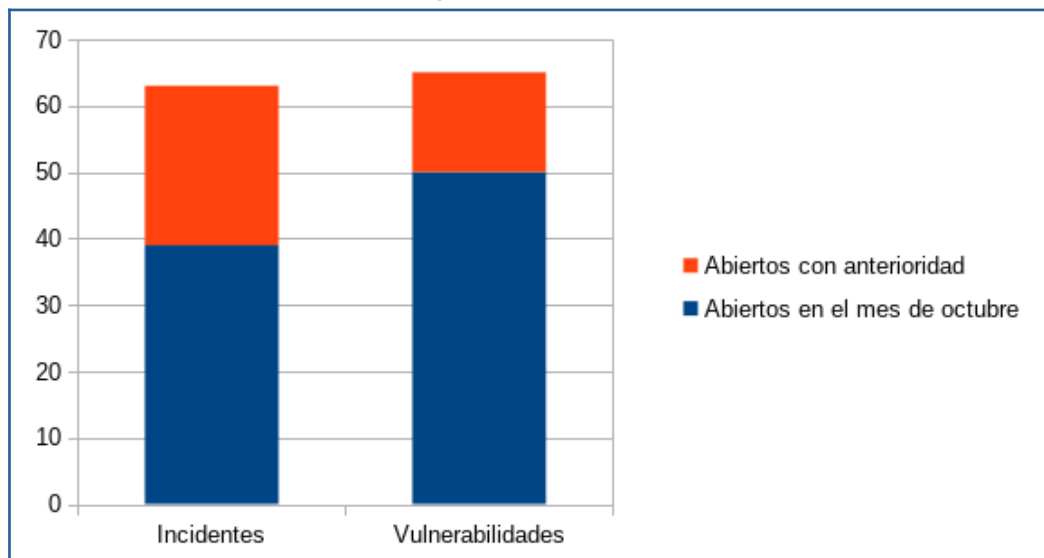
En el mes de octubre, se gestionaron 128 tickets, los cuales representan incidentes y vulnerabilidades, 89 fueron abiertos en octubre y 39 corresponden a meses anteriores; en la siguiente tabla se podrá apreciar la información desagregada:

*Tabla 1: Detalle de tickets abiertos*

Tipo	Tickets	Cantidad
Vulnerabilidades	Abiertos en el mes de octubre	50
	Abiertos con anterioridad	15
Incidentes	Abiertos en el mes de octubre	39
	Abiertos con anterioridad	24
<b>Totales</b>	<b>Tickets abiertos</b>	<b>128</b>

En el siguiente gráfico se puede observar la distribución porcentual de tickets abiertos de incidentes y vulnerabilidades en octubre:

*Gráfico 1: Tickets abiertos*



## 4.2. Tickets abiertos por categoría

### 4.2.1 Incidentes

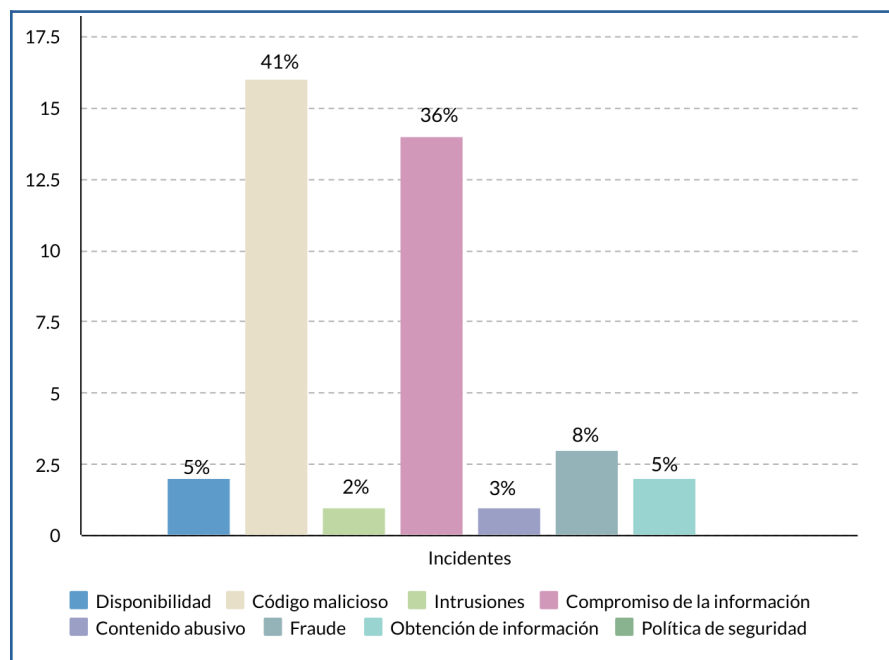
En octubre se registraron 39 tickets nuevos de incidentes, que han sido categorizados de acuerdo al detalle representado por la siguiente tabla y su respectivo gráfico:

Tabla 2: Tickets de incidentes por categoría

Categoría	Tickets	Porcentaje
Disponibilidad	2	5 %
Código malicioso	16	41 %
Intrusiones	1	2 %
Compromiso de la información	14	36 %
Contenido abusivo	1	3 %
Fraude	3	8 %
Obtención de información	2	5 %
Política de seguridad	0	0 %
<b>Totales</b>	<b>39</b>	<b>100 %</b>

Dentro de la categoría **código malicioso** que cuenta con la mayor cantidad de tickets, se gestionaron casos de malware distribuido a través de correos electrónicos en archivos adjuntos.

Gráfico 2: Tickets de incidentes por categoría



#### 4.2.2 Vulnerabilidades

Durante octubre se registraron 50 tickets nuevos de vulnerabilidades, que han sido categorizados de acuerdo a detalle de la siguiente tabla y su gráfico:

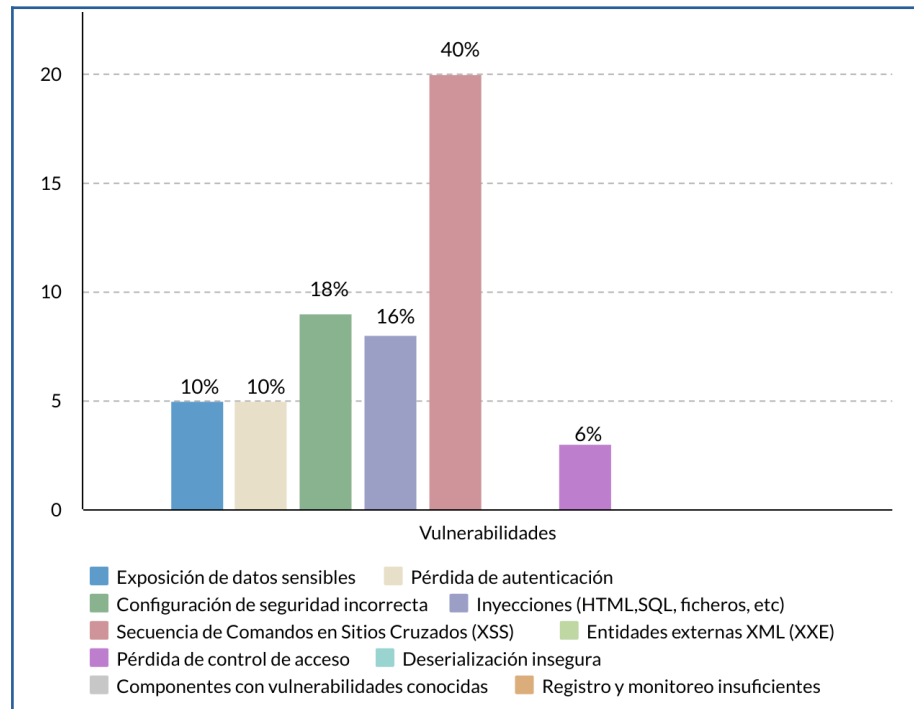
Tabla 3: Tickets de vulnerabilidades por categoría

Categoría	Tickets	Porcentaje
Exposición de datos sensibles	5	10 %
Pérdida de autenticación	5	10 %
Configuración de seguridad incorrecta	9	18 %
Inyecciones (HTML,SQL, ficheros)	8	16 %
Secuencia de Comandos en Sitios Cruzados (XSS)	20	40 %
Entidades externas XML (XXE)	0	0 %
Pérdida de control de acceso	3	6 %
Deserialización insegura	0	0 %
Componentes con vulnerabilidades conocidas	0	0 %
Registro y monitoreo insuficientes	0	0 %
<b>Totales</b>	<b>50</b>	<b>100%</b>

Como se aprecia en la gráfica, la vulnerabilidad de **secuencia de comandos en sitios cruzados reflejados y persistentes**, predominó durante el mes de octubre seguido de la **configuración de seguridad incorrecta** presentes en sistemas de información de entidades del sector público.



Gráfico 3: Tickets de vulnerabilidades por categoría



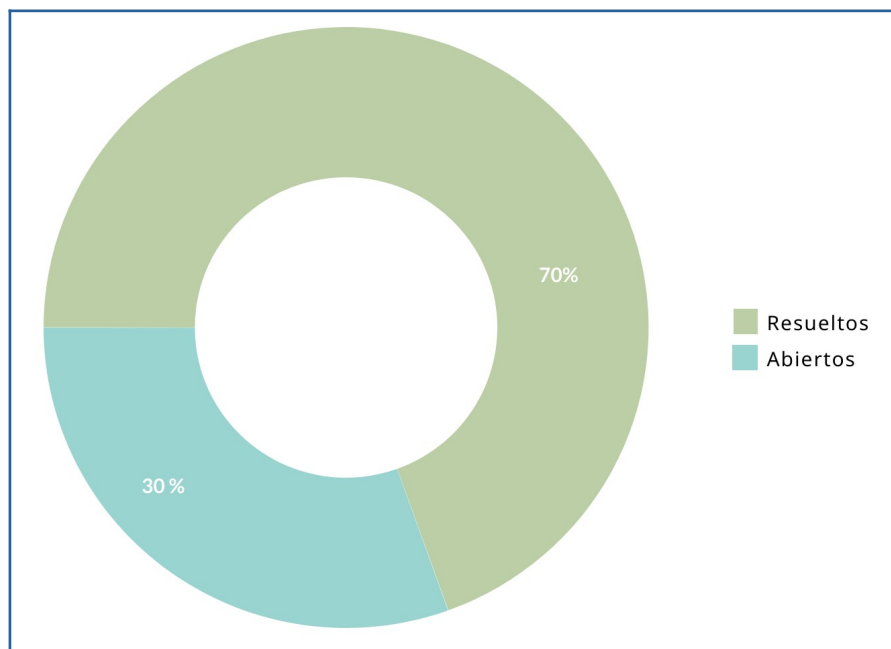
### 4.3. Tickets resueltos

Como resultado de las actividades de gestión de incidentes y vulnerabilidades en octubre, el CGII resolvió 89 tickets, por lo que quedan pendientes de solución para el siguiente mes 39 tickets, a los cuales se está dando el seguimiento respectivo para su solución y posterior cierre. Estos datos se aprecian en la siguiente tabla y su gráfico:

Tabla 4: Tickets abiertos y resueltos

Estado	Tickets	Porcentaje
Resueltos	89	70%
Abiertos (En curso)	39	30%
<b>Totales</b>	<b>128</b>	<b>100%</b>

Gráfico 4: Porcentaje de tickets resueltos



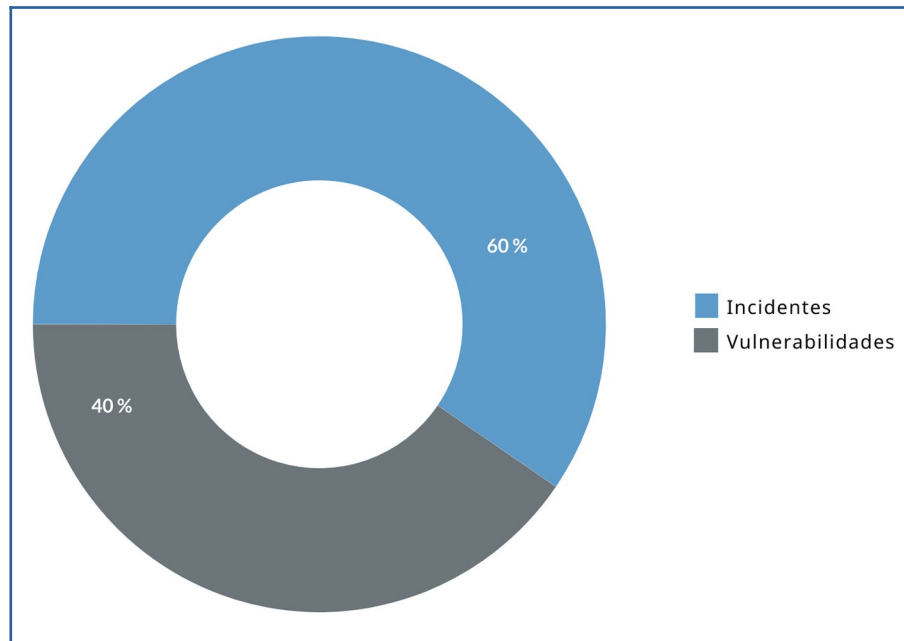
#### 4.4. Tickets resueltos por vulnerabilidad e incidente

Del total de tickets resueltos en el mes de octubre, 53 corresponden a incidentes y 36 a vulnerabilidades, información que se puede observar en la siguiente tabla y su correspondiente gráfico:

*Tabla 5: Tickets resueltos por vulnerabilidad e incidente*

Tipo	Tickets	Porcentaje
Incidentes	53	60%
Vulnerabilidades	36	40%
<b>Totales</b>	<b>89</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 pueden debilitar las defensas de las aplicaciones 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.

**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. Las entidades externas pueden utilizarse para 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 permiten a los atacantes mantener el ataque en el tiempo, pivotear 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.

**Ticket abierto.-** Reporte de un incidente o vulnerabilidad que fue validado y se encuentra en proceso de resolución.

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

**Vulnerabilidad.-** Debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad.



## 6. Historial de cambios

Versión	Fecha	Autor	Descripción	Motivo de cambios
1.0	04/11/2020	Krissia Ferreira	Elaboración	Datos iniciales
1.0	04/11/2020	Franz Rojas	Revisión	Estructura y datos
1.0	09/11/2020	Lizeth Tapia	Revisión	Redacción
1.0	09/11/2020	Ismael Delgado	Aprobación	Aprobación