Taller levantamiento datos empresa,

en seguridad de la información.

Presentado por:

NATALIA VELÁSQUEZ MAHECHA  
ANDRÉS FELIPE RINCÓN MEJÍA  
JANEL JAVIER MOLINA GÓNGORA

Director:

OSCAR ALEJANDRO BUENDIA GODOY

INSTITUCIÓN UNIVERSITARIA UNINPAHU

FACULTAD DE INGENIERÍA Y TECNOLOGÍAS DE LA INFORMACIÓN

COLOMBIA, 2021

**TABLA DE CONTENIDO**

[1. Descripción de la empresa 3](#_Toc67598355)

[2. Evaluación de riesgo 5](#_Toc67598356)

[3. Identificación de los activos 8](#_Toc67598357)

[3.1 Levantamiento de activos – Equipos informáticos 8](#_Toc67598358)

[4. Identificación de amenazas y vulnerabilidades 8](#_Toc67598359)

[5. Reporte de Incidentes 8](#_Toc67598360)

# Descripción de la empresa

Olimpia Management S.A.S es una empresa colombiana de base tecnológica que desarrolla plataformas para la protección y la transformación digital de los países y las empresas, con soluciones innovadoras de comercio electrónico, ciberseguridad y servicios ciudadanos.

Ofrece algunos servicios tecnológicos donde se destacan:

* Trámite para licencia de conducción

Milicencia.co es una plataforma especializada en la gestión de la licencia de conducción donde podrás pagar los pines para la expedición y renovación del pase, consultar la ubicación de los Centros de Reconocimiento y de Enseñanza Automovilística y consultar información útil para cumplir este trámite ciudadano.

* Carpeta ciudadana

Servicio en el cual los ciudadanos pueden recibir, custodiar y compartir de manera segura y confiable documentos digitales, generados en la interacción con personas, entidades públicas y privadas.

* Identidad digital

Identifica digitalmente a tus clientes disminuyendo la desconfianza y agilizando el proceso. Tus usuarios tendrán una experiencia que reduce significativamente el tiempo en ingreso, registro y el uso de claves.

Además, tiene varias plataformas al servicio de los clientes, tales como:

* Identificación de Clientes
* Recaudo Digital
* Factura Electrónica
* Datos Multimedia - Video As a Service
* Sistema para el Control y Vigilancia SISEC



# Evaluación de riesgo





# Identificación de los activos

## Levantamiento de activos – Equipos informáticos

# Identificación de amenazas y vulnerabilidades

# REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Hora de notificación: 10 am

Fecha de notificación: 10/03/2021

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: | | |
| Sede: | | Área / Dependencia: |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: | | Hora en que observó el incidente: | |
| Marque con una cruz todas las opciones que considere aplicables. | | | |
|  | Uso indebido de información crítica. |  | Ingeniería social, fraude o phishing. |
|  | Uso prohibido de un recurso informático o de red. |  | Modificación no autorizada de un sitio o página web |
|  |  |
|  | Divulgación no autorizada de información personal. |  | Eliminación insegura de información. |
|  | Intrusión física. |  | Modificación o eliminación no autorizada de datos. |
|  | Destrucción no autorizada de información. |  | Anomalía o vulnerabilidad técnica de software. |
|  | Robo o pérdida de información. |  | Amenaza o acoso por medio electrónico. |
|  | Interrupción prolongada en un sistema o servicio de red. |  | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) |
|  |  |
|  | Modificación, instalación o eliminación no autorizada de software. |  | Robo o pérdida de un recurso informático. |
|  |  |
|  | Acceso o intento de acceso no autorizado a un sistema informático. |  | Otro no contemplado. Describa: |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente:  **Se utilizaron dispositivos externos infectados con virus maliciosos, que afectaron el buen funcionamiento de los equipos.**  **Se identificó eran virus de tipo informático residentes en la memoria del ordenador.**  **Si el incidente:**   * se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. * se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. * se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de S.I. y reenvíe el mensaje como adjunto a la dirección XXXXXXXXXXXXXXXX |

|  |
| --- |
| Describa brevemente cómo detectó el incidente: |
| El incidente aún está en progreso: [ ] SI [ ] NO |
| Tiempo estimado de duración del incidente: |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: | | | | |
| Localización física: | | | | |
| Describa brevemente la información contenida en el sistema / computador: | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? |  | SI |  | NO |
| Sistema operativo: | | | | |

|  |
| --- |
| **OTROS CONTACTOS** |
| Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente: |
| Apellido y nombres:  Datos de contacto: |
| Apellido y nombres:  Datos de contacto: |

# 

Hora de notificación:

Fecha de notificación:

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: | | |
| Sede: | | Área / Dependencia: |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: | | Hora en que observó el incidente: | |
| Marque con una cruz todas las opciones que considere aplicables. | | | |
|  | Uso indebido de información crítica. |  | Ingeniería social, fraude o phishing. |
|  | Uso prohibido de un recurso informático o de red. |  | Modificación no autorizada de un sitio o página web |
|  |  |
|  | Divulgación no autorizada de información personal. |  | Eliminación insegura de información. |
|  | Intrusión física. |  | Modificación o eliminación no autorizada de datos. |
|  | Destrucción no autorizada de información. |  | Anomalía o vulnerabilidad técnica de software. |
|  | Robo o pérdida de información. |  | Amenaza o acoso por medio electrónico. |
|  | Interrupción prolongada en un sistema o servicio de red. |  | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) |
|  |  |
|  | Modificación, instalación o eliminación no autorizada de software. |  | Robo o pérdida de un recurso informático. |
|  |  |
|  | Acceso o intento de acceso no autorizado a un sistema informático. |  | Otro no contemplado. Describa: |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente:  **Se accedió a un link de activación de la licencia el cual contenia un malwere que lo penetrar en la red.**  **Si el incidente:**   * se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. * se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. * se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de S.I. y reenvíe el mensaje como adjunto a la dirección XXXXXXXXXXXXXXXX |

|  |
| --- |
| Describa brevemente cómo detectó el incidente: |
| El incidente aún está en progreso: [ ] SI [ ] NO |
| Tiempo estimado de duración del incidente: |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: | | | | |
| Localización física: | | | | |
| Describa brevemente la información contenida en el sistema / computador: | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? |  | SI |  | NO |
| Sistema operativo: | | | | |

|  |
| --- |
| **OTROS CONTACTOS** |
| Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente: |
| Apellido y nombres:  Datos de contacto: |
| Apellido y nombres:  Datos de contacto: |

Hora de notificación:

Fecha de notificación:

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: | | |
| Sede: | | Área / Dependencia: |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: | | Hora en que observó el incidente: | |
| Marque con una cruz todas las opciones que considere aplicables. | | | |
|  | Uso indebido de información crítica. |  | Ingeniería social, fraude o phishing. |
|  | Uso prohibido de un recurso informático o de red. |  | Modificación no autorizada de un sitio o página web |
|  |  |
|  | Divulgación no autorizada de información personal. |  | Eliminación insegura de información. |
|  | Intrusión física. |  | Modificación o eliminación no autorizada de datos. |
|  | Destrucción no autorizada de información. |  | Anomalía o vulnerabilidad técnica de software. |
|  | Robo o pérdida de información. |  | Amenaza o acoso por medio electrónico. |
|  | Interrupción prolongada en un sistema o servicio de red. |  | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) |
|  |  |
|  | Modificación, instalación o eliminación no autorizada de software. |  | Robo o pérdida de un recurso informático. |
|  |  |
|  | Acceso o intento de acceso no autorizado a un sistema informático. |  | Otro no contemplado. Describa: |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente:  **No se logró identificar el ataque cibernético que afecto grandes compañías con secuestro de información por la indisponibilidad de uno de los servidores.**  **Si el incidente:**   * se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. * se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. * se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de S.I. y reenvíe el mensaje como adjunto a la dirección XXXXXXXXXXXXXXXX |

|  |
| --- |
| Describa brevemente cómo detectó el incidente: |
| El incidente aún está en progreso: [ ] SI [ ] NO |
| Tiempo estimado de duración del incidente: |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: | | | | |
| Localización física: | | | | |
| Describa brevemente la información contenida en el sistema / computador: | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? |  | SI |  | NO |
| Sistema operativo: | | | | |

|  |
| --- |
| **OTROS CONTACTOS** |
| Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente: |
| Apellido y nombres:  Datos de contacto: |
| Apellido y nombres:  Datos de contacto: |

Hora de notificación:

Fecha de notificación:

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: | | |
| Sede: | | Área / Dependencia: |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: | | Hora en que observó el incidente: | |
| Marque con una cruz todas las opciones que considere aplicables. | | | |
|  | Uso indebido de información crítica. |  | Ingeniería social, fraude o phishing. |
|  | Uso prohibido de un recurso informático o de red. |  | Modificación no autorizada de un sitio o página web |
|  |  |
|  | Divulgación no autorizada de información personal. |  | Eliminación insegura de información. |
|  | Intrusión física. |  | Modificación o eliminación no autorizada de datos. |
|  | Destrucción no autorizada de información. |  | Anomalía o vulnerabilidad técnica de software. |
|  | Robo o pérdida de información. |  | Amenaza o acoso por medio electrónico. |
|  | Interrupción prolongada en un sistema o servicio de red. |  | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) |
|  |  |
|  | Modificación, instalación o eliminación no autorizada de software. |  | Robo o pérdida de un recurso informático. |
|  |  |
|  | Acceso o intento de acceso no autorizado a un sistema informático. |  | Otro no contemplado. Describa: |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente:  **Se logró vulnerar la seguridad de la base de datos debido al acceso de múltiples usuarios con las mismas credenciales.**  **Si el incidente:**   * se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. * se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. * se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de S.I. y reenvíe el mensaje como adjunto a la dirección XXXXXXXXXXXXXXXX |

|  |
| --- |
| Describa brevemente cómo detectó el incidente: |
| El incidente aún está en progreso: [ ] SI [ ] NO |
| Tiempo estimado de duración del incidente: |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: | | | | |
| Localización física: | | | | |
| Describa brevemente la información contenida en el sistema / computador: | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? |  | SI |  | NO |
| Sistema operativo: | | | | |

|  |
| --- |
| **OTROS CONTACTOS** |
| Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente: |
| Apellido y nombres:  Datos de contacto: |
| Apellido y nombres:  Datos de contacto: |

Hora de notificación:

Fecha de notificación:

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: | | |
| Sede: | | Área / Dependencia: |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: | | Hora en que observó el incidente: | |
| Marque con una cruz todas las opciones que considere aplicables. | | | |
|  | Uso indebido de información crítica. |  | Ingeniería social, fraude o phishing. |
|  | Uso prohibido de un recurso informático o de red. |  | Modificación no autorizada de un sitio o página web |
|  |  |
|  | Divulgación no autorizada de información personal. |  | Eliminación insegura de información. |
|  | Intrusión física. |  | Modificación o eliminación no autorizada de datos. |
|  | Destrucción no autorizada de información. |  | Anomalía o vulnerabilidad técnica de software. |
|  | Robo o pérdida de información. |  | Amenaza o acoso por medio electrónico. |
|  | Interrupción prolongada en un sistema o servicio de red. |  | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) |
|  |  |
|  | Modificación, instalación o eliminación no autorizada de software. |  | Robo o pérdida de un recurso informático. |
|  |  |
|  | Acceso o intento de acceso no autorizado a un sistema informático. |  | Otro no contemplado. Describa: |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente:  **Ingreso de personal no autorizado por fallas en el dispositivo biométrico.**  **Si el incidente:**   * se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. * se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. * se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de S.I. y reenvíe el mensaje como adjunto a la dirección XXXXXXXXXXXXXXXX |

|  |
| --- |
| Describa brevemente cómo detectó el incidente: |
| El incidente aún está en progreso: [ ] SI [ ] NO |
| Tiempo estimado de duración del incidente: |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: | | | | |
| Localización física: | | | | |
| Describa brevemente la información contenida en el sistema / computador: | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? |  | SI |  | NO |
| Sistema operativo: | | | | |

|  |
| --- |
| **OTROS CONTACTOS** |
| Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente: |
| Apellido y nombres:  Datos de contacto: |
| Apellido y nombres:  Datos de contacto: |

Hora de notificación:

Fecha de notificación:

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: | | |
| Sede: | | Área / Dependencia: |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: | | Hora en que observó el incidente: | |
| Marque con una cruz todas las opciones que considere aplicables. | | | |
|  | Uso indebido de información crítica. |  | Ingeniería social, fraude o phishing. |
|  | Uso prohibido de un recurso informático o de red. |  | Modificación no autorizada de un sitio o página web |
|  |  |
|  | Divulgación no autorizada de información personal. |  | Eliminación insegura de información. |
|  | Intrusión física. |  | Modificación o eliminación no autorizada de datos. |
|  | Destrucción no autorizada de información. |  | Anomalía o vulnerabilidad técnica de software. |
|  | Robo o pérdida de información. |  | Amenaza o acoso por medio electrónico. |
|  | Interrupción prolongada en un sistema o servicio de red. |  | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) |
|  |  |
|  | Modificación, instalación o eliminación no autorizada de software. |  | Robo o pérdida de un recurso informático. |
|  |  |
|  | Acceso o intento de acceso no autorizado a un sistema informático. |  | Otro no contemplado. Describa: |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente:  **Si el incidente:**   * se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. * se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. * se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con el Depto. de S.I. y reenvíe el mensaje como adjunto a la dirección XXXXXXXXXXXXXXXX |

|  |
| --- |
| Describa brevemente cómo detectó el incidente: |
| El incidente aún está en progreso: [ ] SI [ ] NO |
| Tiempo estimado de duración del incidente: |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: | | | | |
| Localización física: | | | | |
| Describa brevemente la información contenida en el sistema / computador: | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? |  | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? |  | SI |  | NO |
| Sistema operativo: | | | | |

|  |
| --- |
| **OTROS CONTACTOS** |
| Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente: |
| Apellido y nombres:  Datos de contacto: |
| Apellido y nombres:  Datos de contacto: |

# 