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](#_Toc69492529)

[2. Evaluación de riesgo 5](#_Toc69492530)

[3. Identificación de los activos 8](#_Toc69492531)

[3.1 Levantamiento de activos – Equipos informático 8](#_Toc69492532)

[3.2 Levantamiento de activos – Servicios 12](#_Toc69492533)

[3.3 Levantamiento de activos – Equipos informáticos 12](#_Toc69492534)

[3.4 Levantamiento de activos – Redes de comunicación 12](#_Toc69492535)

[3.5 Levantamiento de activos – Instalaciones 12](#_Toc69492536)

[3.6 Levantamiento de activos – Personas 12](#_Toc69492537)

[4. Identificación de amenazas y vulnerabilidades 12](#_Toc69492538)

[5. Reporte de Incidentes 13](#_Toc69492539)

# 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

Anexo archivo Excel Matriz Riesgo Olimpia.XLSX

# Identificación de los activos

## Levantamiento de activos – Aplicaciones

Nombre: María Del Pilar Ruiz

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO: APL01 | NOMBRE: Visual Studio |
| DESCRIPCION: Es un entorno de desarrollo integrado (IDE) la cual permite a los desarrolladores crear las aplicaciones o servicios que solicitan los clientes. | |
| RESPONSABLE: María Del Pilar Ruiz | |
| TIPO: Entorno de desarrollo integrado | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy alto | Ya que si no se tiene disponible la aplicación no se podrá dar cumplimiento con los requerimientos de los clientes puesto que no se podrían desarrollar los requerimientos |
| INTEGRIDAD | Alto | La pérdida de integridad afectaría con los objetivos y entregas de la compañía |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente los procesos de la compañía |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Felipe Ruiz

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO: APL02 | NOMBRE: Azure |
| DESCRIPCION: Es el servicio de computación en la nube | |
| RESPONSABLE: Felipe Ruiz | |
| TIPO: Computación en la nube software | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Ya que si no se tiene disponible la aplicación no se podrá tener un buen manejo de almacenamiento de la información o aplicaciones. |
| INTEGRIDAD | Alto | La pérdida de integridad afectaría la calidad del almacenamiento de la información |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente los procesos de la compañía |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Juan López

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO: APL03 | NOMBRE: Aranda |
| DESCRIPCION: Esta plataforma facilita el manejo y el control de todos los requerimientos que solicitan los clientes. | |
| RESPONSABLE: Juan López | |
| TIPO: | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Ya que si no se tiene disponible la aplicación no se podrá tener un buen control sobre los requerimientos solicitados por los clientes. |
| INTEGRIDAD | Alto | La pérdida de integridad afectaría la calidad sobre el control de los requerimientos solicitados. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente los procesos de la compañía |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Juan López

Departamento: Recursos humanos

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO: APL04 | NOMBRE: Heinsohn human |
| DESCRIPCION: Aplicación en la cual se lleva la administración del personal, liquidación de nómina, implementación de sistemas de información especializado en administración de nómina y gestión humana. | |
| RESPONSABLE: Juan López | |
| TIPO: Contabilidad | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Ya que si no se tiene disponible la aplicación no se podrá tener un buen control sobre las nóminas de los empleados y los procesos que realiza el área de recursos humanos |
| INTEGRIDAD | Alto | La pérdida de integridad afectaría la calidad del almacenamiento de la información |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente los procesos de la compañía |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: David Rodriguez

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO: APL05 | NOMBRE: Sql server management studio |
| DESCRIPCION: Es la herramienta principal para la gestión de bases de datos SQL Serve | |
| RESPONSABLE: David Rodriguez | |
| TIPO: Gestor de base de datos | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy alto | Ya que si no se tiene disponible la aplicación no se podrá dar cumplimiento con los requerimientos de los clientes puesto que no se podrían desarrollar los requerimientos |
| INTEGRIDAD | Alto | La pérdida de integridad afectaría con los objetivos y entregas de la compañía. |
| CONFIDENCIALIDAD | Muy alto | La pérdida de confidencialidad de la información en la aplicación afecta totalmente el desarrollo de los requerimientos. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

## Levantamiento de activos – Servicios

Nombre: Edgar García

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO: CSER-01 | NOMBRE: Factura Electrónica |
| DESCRIPCION: Plataforma para la emisión, envío, recepción de facturas electrónicas incorporando firma digital. | |
| RESPONSABLE: Edgar García | |
| TIPO: Financiera | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Servicio debe estar disponible para los procesos de facturación, que se realizan en cualquier hora. |
| INTEGRIDAD | Muy alto | La información debe ser totalmente confiable. |
| CONFIDENCIALIDAD | Muy alto | Se debe garantizar la total confidencialidad con la información almacenada en el sistema |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Edgar García

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO: CSER-02 | NOMBRE: Recaudo Digital |
| DESCRIPCION: Gestión de cobros y recaudos digitales. Cobra en línea y recibe pagos al instante. | |
| RESPONSABLE: Edgar García | |
| TIPO: Financiera | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | Servicio debe estar disponible para los procesos de recaudo, que se realizan en cualquier hora. |
| INTEGRIDAD | Muy alto | La información debe ser totalmente confiable. |
| CONFIDENCIALIDAD | Muy alto | Se debe garantizar la total confidencialidad con la información almacenada en el sistema y de los pagos realizados. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Edgar García

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO: CSER-03 | NOMBRE: Cámaras térmicas |
| DESCRIPCION: Soluciones digitales para monitoreo de temperatura y control de acceso o circulación | |
| RESPONSABLE: Edgar García | |
| TIPO: Dispositivos | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Servicio debe estar disponible para el monitoreo y control de acceso, que normalmente se realiza en unos horarios preestablecidos |
| INTEGRIDAD | Alto | La información debe ser confiable. |
| CONFIDENCIALIDAD | Medio | Se debe garantizar la confidencialidad con la poca información almacenada en el sistema |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Diego Zabaleta

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO: CSER-04 | NOMBRE: Reconoser validación de identidad multi-biométrica (abis) |
| DESCRIPCION: ReconoSer Multi-biométria, hace uso de las tecnologías más avanzadas para el reconocimiento biométrico de personas a través huellas, rostro y voz. | |
| RESPONSABLE: Diego Zabaleta | |
| TIPO: Reconocimiento biometrico | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Servicio debe estar disponible para los procesos de identificación biometrica, que se normalmente realizan en horarios preestablecidos. |
| INTEGRIDAD | Muy alto | La información debe ser totalmente confiable. |
| CONFIDENCIALIDAD | Muy alto | Se debe garantizar la total confidencialidad con la información sensible almacenada en el sistema |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Joaquin Escarraga

Departamento: Desarrollo

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO: CSER-05 | NOMBRE: SISEC CEA |
| DESCRIPCION: Sistema desarrollado para los CEA (Centros de Enseñanza Automovilística), para la validación de identidad y el control de asistencia a las clases de los aspirantes para obtener una licencia de conducción a través de un curso teórico práctico. | |
| RESPONSABLE: Joaquin Escarraga | |
| TIPO: | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Servicio debe estar disponible para los procesos de validación de identidad de los aspirantes, que normalmente se realizan en horarios preestablecidos. |
| INTEGRIDAD | Muy alto | La información debe ser totalmente confiable. |
| CONFIDENCIALIDAD | Muy alto | Se debe garantizar la total confidencialidad con la información almacenada en el sistema |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

## Levantamiento de activos – Equipos informáticos

Nombre: Ingrid Vélez

Departamento: Sistemas

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO: EI01 | NOMBRE: Computadores Escritorios |
| DESCRIPCION: Equipos de oficina | |
| RESPONSABLE: Ingrid Vélez | |
| UBICACIÓN: Oficinas | |
| NUMERO: 10 | |
| TIPO: Computo | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 4 | La falta de disponibilidad de los equipos de cómputo bloquearía la actividad del área de administración. |
| INTEGRIDAD | 3 | La pérdida de integridad de integridad de los equipos de cómputo afecta el área de administración. |
| CONFIDENCIALIDAD | 5 | La pérdida de confidencialidad de la información de los equipos del área de administración afecta totalmente la actividad de la operación. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: Si | grado: Alto |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Ingrid Vélez

Departamento: Sistemas

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO: EI02 | NOMBRE: Computadores portátiles |
| DESCRIPCION: Equipos de desarrollo | |
| RESPONSABLE: Ingrid Vélez | |
| UBICACIÓN: Oficinas | |
| NUMERO: 15 | |
| TIPO: Computo | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 5 | La falta de disponibilidad de los equipos de cómputo bloquearía la actividad del área de desarrollo. |
| INTEGRIDAD | 4 | La pérdida de integridad de los equipos de cómputo afecta considerablemente el área de desarrollo. |
| CONFIDENCIALIDAD | 5 | La pérdida de confidencialidad de la información de los equipos del área de desarrollo afecta totalmente la actividad de la operación. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Ingrid Vélez

Departamento: Sistemas

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO: EI03 | NOMBRE: Impresoras |
| DESCRIPCION: Equipos de oficina | |
| RESPONSABLE: Ingrid Vélez | |
| UBICACIÓN: Oficinas | |
| NUMERO: 2 | |
| TIPO: Computo | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 2 | La falta de disponibilidad de los equipos de tecnología afecta de cierta manera la actividad del área de administración. |
| INTEGRIDAD | 2 | La pérdida de integridad de los equipos de tecnología afecta de cierta manera el área de administración. |
| CONFIDENCIALIDAD | 2 | La pérdida de confidencialidad de la información de los equipos de tecnología afecta de cierta manera la actividad de la operación. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Ingrid Vélez

Departamento: Sistemas

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO: EI04 | NOMBRE: Teléfonos |
| DESCRIPCION: Equipos de oficina | |
| RESPONSABLE: Ingrid Vélez | |
| UBICACIÓN: Oficinas | |
| NUMERO: 8 | |
| TIPO: Computo | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 1 | La falta de disponibilidad de los equipos de telefonía afecta de forma casi imperceptible de las actividades del área de administración. |
| INTEGRIDAD | 1 | La pérdida de integridad de los equipos de telefonía afecta de forma casi imperceptible el área de administración. |
| CONFIDENCIALIDAD | 1 | La pérdida de confidencialidad de la información de los equipos de telefonía del área de administración afecta de forma casi imperceptible la actividad de la operación. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Ingrid Vélez

Departamento: Sistemas

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO: EI05 | NOMBRE: Discos |
| DESCRIPCION: Disco de Backup | |
| RESPONSABLE: Ingrid Vélez | |
| UBICACIÓN: Oficinas | |
| NUMERO: 10 | |
| TIPO: Computo | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 4 | La falta de disponibilidad de los equipos de telefonía afecta de forma casi imperceptible de las actividades del área de administración. |
| INTEGRIDAD | 5 | La pérdida de integridad de los equipos de telefonía afecta de forma casi imperceptible el área de administración. |
| CONFIDENCIALIDAD | 5 | La pérdida de confidencialidad de la información de los equipos de telefonía del área de administración afecta de forma casi imperceptible la actividad de la operación. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

## Levantamiento de activos – Redes de comunicación

Nombre: Carlos Gonzales  
Departamento: Desarrollo

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: RED01 | NOMBRE: Conexión LAN |
| DESCRIPCION: Esta conexión se hace por medio de un cable ethernet. | |
| RESPONSABLE: Carlos Gonzales | |
| UBICACIÓN: Oficinas de desarrollo | |
| NUMERO: | |
| TIPO: Red Área local | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La falta de disponibilidad de esta conexión no se es posible realizar los proyectos y conexiones de los empleados. |
| INTEGRIDAD | Alto | La falta de integridad afecta la operación de los procesos de la compañía. |
| CONFIDENCIALIDAD | Alto | La perdida de confidencialidad afecta las conexiones hacia los equipos. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Jessica Rodríguez  
Departamento: Soporte

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: RED02 | NOMBRE: Red telefónica soporte interno |
| DESCRIPCION: A esta línea se comunican las personas directas de la compañía para solicitar soporte ya sea mantenimiento, apoyo en procesos. | |
| RESPONSABLE: Jessica Rodríguez | |
| UBICACIÓN: Área de soporte. | |
| NUMERO: | |
| TIPO: Red telefónica | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Baja | La pérdida de disponibilidad afecta de cierta forma los procesos de la compañía |
| INTEGRIDAD | Alto | La falta de integridad afecta la operación de los procesos de la compañía. |
| CONFIDENCIALIDAD | Medio | La pérdida de confidencialidad afecta la comunicación. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Heidy Ortiz

Departamento: Sistemas

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: RED03 | NOMBRE: Red telefónica PBX |
| DESCRIPCION: Es una red telefónica privada utilizada dentro de una empresa. | |
| RESPONSABLE: Heidy Ortiz | |
| UBICACIÓN: En cada una de las oficinas de la compañía | |
| NUMERO: | |
| TIPO: Red Telefónica | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Baja | La pérdida de disponibilidad afecta de cierta forma los procesos de la compañía |
| INTEGRIDAD | Alto | La falta de integridad afecta la operación de los procesos de la compañía. |
| CONFIDENCIALIDAD |  |  |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Andrea Ramírez

Departamento: CallCenter

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: RED04 | NOMBRE: Red telefónica de atención al cliente |
| DESCRIPCION: Línea telefónica para recibir las llamabas de los clientes, o realizar soporte. | |
| RESPONSABLE: Andrea Ramírez | |
| UBICACIÓN: CallCenter | |
| NUMERO: | |
| TIPO: Línea Telefónica | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alta | La pérdida de disponibilidad afecta totalmente que los clientes no tengan un soporte. |
| INTEGRIDAD | Alto | La falta de integridad afecta la operación de los procesos de la compañía. |
| CONFIDENCIALIDAD |  |  |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Miguel Hernández

Departamento:

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: RED05 | NOMBRE: VPN |
| DESCRIPCION: Cada uno de los empleados maneja la conexión al equipo por medio de una VPN esto para proteger la información y así evitar el fácil acceso de los hackers. | |
| RESPONSABLE: Miguel Hernández | |
| UBICACIÓN: En todos lo equipos de los desarrolladores. | |
| NUMERO: | |
| TIPO: | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La falta de disponibilidad de esta conexión afecta totalmente a las conexiones de los empleados. |
| INTEGRIDAD | Alto | La falta de integridad afecta la operación de los procesos de la compañía. |
| CONFIDENCIALIDAD |  |  |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

## Levantamiento de activos – Instalaciones

Nombre: Daniel Medina

Departamento: Gerencia

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO: CINT-01 | NOMBRE: Oficina Administrativa |
| DESCRIPCION: Edificio donde labora todo el equipo administrativo y de recursos humanos, y cuenta con un espacio para 125 personas. | |
| RESPONSABLE: Daniel Medina | |
| UBICACIÓN: Calle. 24 #7-18 | |
| NUMERO: 7425133 | |
| TIPO: Edificio | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Se encuentra disponible en unos horarios preestablecidos |
| INTEGRIDAD | Medio | Debe garantizar la integridad del edificio para recibir a sus funcionarios y visitantes |
| CONFIDENCIALIDAD | Medio | Es de fácil conocimiento por los demás para su acceso |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Daniel Medina

Departamento: Gerencia

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO: CINT-02 | NOMBRE: Oficina Comercial |
| DESCRIPCION: Edificio donde labora todo el equipo comercial y se recibe a los clientes y visitantes, y cuenta con un espacio para 88 personas. | |
| RESPONSABLE: Daniel Medina | |
| UBICACIÓN: Avenida El Dorado #69 - 51, B Piso 2 Of. 202 | |
| NUMERO: 7425133 | |
| TIPO: Edificio | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Se encuentra disponible en unos horarios preestablecidos |
| INTEGRIDAD | Medio | Debe garantizar la integridad del edificio para recibir a sus funcionarios y clientes |
| CONFIDENCIALIDAD | Medio | Es de fácil conocimiento por los demás para su acceso |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Ivan Canro

Departamento: Gerencia

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO: CINT-03 | NOMBRE: Wework |
| DESCRIPCION: Edificio donde labora todo el equipo de desarrollo, y cuenta con un espacio para 185 personas. | |
| RESPONSABLE: Ivan Canro | |
| UBICACIÓN: Calle 26 # 92-32 | |
| NUMERO: 7425133 | |
| TIPO: Edificio | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | Se encuentra disponible en unos horarios preestablecidos pero con disponibilidad adicional en caso de ser necesario continua con las operaciones |
| INTEGRIDAD | Medio | Debe garantizar la integridad del edificio para recibir a sus funcionarios y visitantes |
| CONFIDENCIALIDAD | Medio | Es de fácil conocimiento por los demás para su acceso |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Sergio Montoya

Departamento: IT

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO: CINT-04 | NOMBRE: Datacenter |
| DESCRIPCION: infraestructura física utilizada para alojar sistemas informáticos que procesan información sensible. | |
| RESPONSABLE: Sergio Montoya | |
| UBICACIÓN: Calle 26 # 92-32 | |
| NUMERO: 7425133 | |
| TIPO: Infraestructura | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | Se debe garantizar total disponibilidad con algunos servidores de respaldo para garantizar el funcionamiento de los diferentes sistemas de la compañía. |
| INTEGRIDAD | Muy Alto | Debe garantizar la total integridad de la información que se maneja y distribuye a través de las diferentes plataformas. |
| CONFIDENCIALIDAD | Muy Alto | Se debe garantizar la total confidencialidad con la información sensible almacenada en el sistema |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

Nombre: Iván Canro

Departamento: recursos humanos

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO: CINT-05 | NOMBRE: Zona común Wework |
| DESCRIPCION: Zona común donde se reúnen el equipo de desarrollo con los demás funcionarios de otras empresas que se encuentran allí | |
| RESPONSABLE: Daniel Medina | |
| UBICACIÓN: Calle. 24 #7-18 | |
| NUMERO: 7425133 | |
| TIPO: Edificio | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | Se encuentra disponible en unos horarios preestablecidos |
| INTEGRIDAD | Medio | Debe garantizar la integridad del edificio para recibir a sus funcionarios y visitantes |
| CONFIDENCIALIDAD | Medio | Es de fácil conocimiento por los demás para su acceso |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

FIRMA DE ACEPTACION

## Levantamiento de activos – Personas

Nombre: Dayana Salgado

Departamento: Administración

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO: AP01 | NOMBRE: Recepcionista |
| DESCRIPCION: Brindar atención al personal interno y externo en sus requerimientos, Manejo de la planta telefónica y direccionamiento adecuado de mensajes. | |
| RESPONSABLE: Dayana Salgado | |
| UBICACIÓN: Oficinas - Recepción | |
| NUMERO: 1 | |
| TIPO: Administración | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 4 | La falta de disponibilidad de la persona indicada implica una coordinación adecuada con las actividades varias. |
| INTEGRIDAD | 4 | La pérdida de integridad de la persona indicada afecta considerablemente el área administrativa. |
| CONFIDENCIALIDAD | 5 | La pérdida de confidencialidad de la información del área afecta de considerablemente la actividad de la operación. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Santiago Mendez

Departamento: Desarrollador De Software

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO: AP02 | NOMBRE: Desarrollador De Software Senior |
| DESCRIPCION: Codificar los requerimientos recibidos por parte de los Jefes de Desarrollo. Realizar mejoras incrementales a las funcionalidades asignadas. Realizar las pruebas a las funcionalidades desarrolladas. Realizar la documentación técnica de los módulos asignados. | |
| RESPONSABLE: Santiago Mendez | |
| UBICACIÓN: Oficinas | |
| NUMERO: 4 | |
| TIPO: Desarrollador | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 5 | La falta de disponibilidad implica realizar la actualización de los cronogramas y tareas asignadas de acuerdo a la disponibilidad. |
| INTEGRIDAD | 4 | La pérdida de integridad implica el cumplimiento con los requisitos. |
| CONFIDENCIALIDAD | **5** | La pérdida de confidencialidad de la información implica activamente en los programas y actividades. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Daniel Castro

Departamento: Talento humano

|  |  |
| --- | --- |
| Personas | |
| CODIGO: AP03 | NOMBRE: Asistente De Talento Humano |
| DESCRIPCION: Apoyar la ejecución del plan de formación, apoyar los procedimientos selección y contratación de personal en las etapas que corresponden, suministrar información para el pedido de dotación del personal y realizar su entrega, consolidar y entregar de novedades de nómina. | |
| RESPONSABLE: Daniel Castro | |
| UBICACIÓN: Oficinas | |
| NUMERO: 1 | |
| TIPO: Talento humano | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 5 | La falta de disponibilidad implica la participar activamente en los programas y actividades |
| INTEGRIDAD | 4 | La pérdida de integridad implica a contribuir al  cumplimiento de los procesos y apoyo de las  actividades. |
| CONFIDENCIALIDAD | **5** | La pérdida de confidencialidad de la información implica la calidad del servicio. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Dayana Salgado

Departamento: Administración

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO: AP04 | NOMBRE: Servicios generales |
| DESCRIPCION: Limpiar baños, puestos de trabajo, cocinetas y zonas comunes de cada oficina, preparar el café y aromáticas, botar la basura diariamente, limpiar vidrios, persianas y lámparas, Realizar aseo general semanalmente. | |
| RESPONSABLE: Dayana Salgado | |
| UBICACIÓN: Oficinas | |
| NUMERO: 1 | |
| TIPO: Administración | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 5 | La falta de disponibilidad implica deterioro de los espacios y recursos físicos. |
| INTEGRIDAD | 4 | La pérdida de integridad implica el cumplimiento las actividades establecidas. |
| CONFIDENCIALIDAD | **3** | La pérdida de confidencialidad de la información implica el respeto y confianza en la organización. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

Nombre: Juan Pinzón

Departamento: Comercial

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO: AP05 | NOMBRE: Ejecutivo Comercial |
| DESCRIPCION: Cumplir con los presupuestos e indicadores de ventas establecidos, Alimentar el sistema de información (plataformas) acorde a la gestión comercial que se realiza, elaborar y presentar las cotizaciones a los clientes. | |
| RESPONSABLE: Juan Pinzón | |
| UBICACIÓN: Oficinas | |
| NUMERO: 3 | |
| TIPO: Comercial | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | 5 | La falta de disponibilidad implica en promover el desarrollo de nuevos productos y servicios |
| INTEGRIDAD | 4 | La pérdida de integridad implica establecer comunicación permanente con clientes. |
| CONFIDENCIALIDAD | **5** | La pérdida de confidencialidad de la información implica dar cumplimiento con los requisitos normativos, legales y reglamentarios que rigen la  actividad económica de la organización. |

|  |  |
| --- | --- |
| DEPENDENCIA DE ACTIVOS INFERIORES | |
| activo: | grado: |
| ¿Por qué?: | |

|  |
| --- |
| FIRMA DE ACEPTACION |

# Identificación de amenazas y vulnerabilidades

# Reporte de incidentes 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: Erika Sánchez | | |
| Sede: Bogotá | | Área / Dependencia: |
| Correo electrónico: Erika.Sánchez@outlook.com | | Administración |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: 10/03/2021 | | Hora en que observó el incidente: 10am | |
| 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. |
| X | 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. | X | 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.**  **Un virus llamado Recycler el cual consiste en crear un acceso directo de un programa y eliminar la aplicación original.**  **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:  Se detectó cuando el funcionario fue abrir una aplicación por el acceso directo de esta y ya no se encontraba en la ruta. |
| El incidente aún está en progreso: [ ] SI [ x] NO |
| Tiempo estimado de duración del incidente: 8h |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente:  Un funcionario del área de administración en el cargo de auxiliar administrativo. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada:  Computadora Asignada. | | | | |
| Localización física:  Administración | | | | |
| Describa brevemente la información contenida en el sistema / computador:  Paquete Office (Word, Excel, etc.)  Correo | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? | x | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? | x | SI |  | NO |
| ¿El recurso afectado tiene conexión a Internet? | x | SI |  | NO |
| Sistema operativo: Windows | | | | |

|  |
| --- |
| **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: 3:00 PM

Fecha de notificación: 10/04/2021

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: Sergio Campos | | |
| Sede: Bogotá | | Área / Dependencia: |
| Correo electrónico: Sergio.Campos@outlook.com | | Infraestructura |
| 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. |
|  |  |
| X | 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.**  **Se identificó que los usuarios no tenían permiso para realizar acciones en la base de datos, y se logró inhabilitar los permisos a dicho roles.**  **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:  Al momento de realizar una migración de información se detectó cambios en la información no estipulados con anterioridad determinando un uso indebido de acciones de actualización de data. |
| El incidente aún está en progreso: [ ] SI [ x] NO |
| Tiempo estimado de duración del incidente: 6 Horas |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente:  Ing. Sistemas encargado de migración del área de base de datos. |

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

