**SEGURIDAD INFORMÁTICA**

**SEGUNDO CORTE**

**DANIEL STIVEN GARCIA MIRANDA**

**JAIR CAMILO MADRIGAL TORRES**

**YEFERSON DAVID MURCIA MIRANDA**

**UNINPAHU**

**FACULTAD DE INGENIERIA**

**INGENIERIA DE SOTFWARE**

**GRUPO 800**

**BOGOTÁ-COLOMBIA**

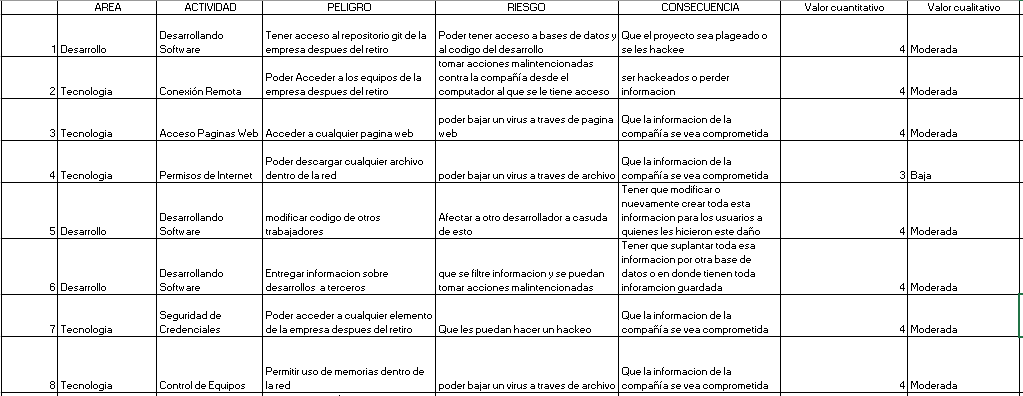
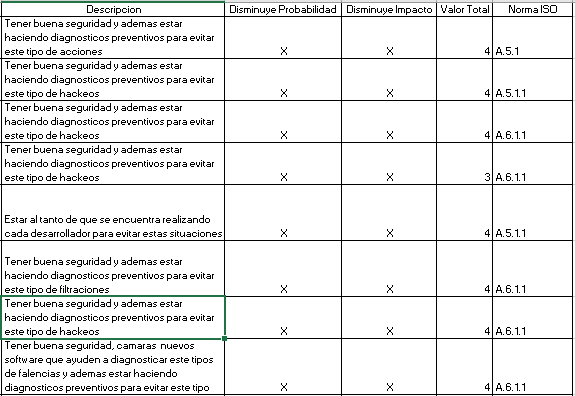
**2021**

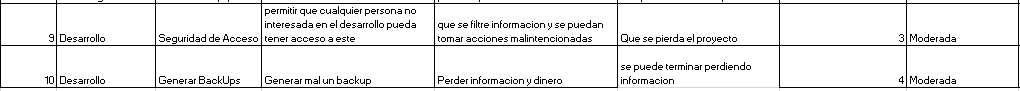
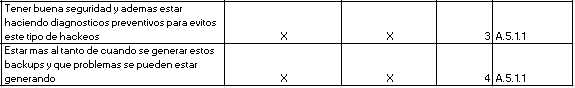
Taller levantamiento Datos Empresa, en Seguridad de la Información.

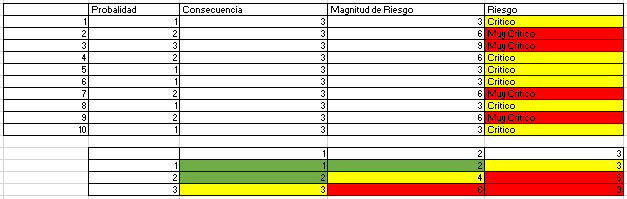
* + 1. **Situación actual de la empresa**

Empresa dedicada desde 2012 a desarrollar soluciones tecnológicas integrales de alta calidad técnica, que inspiran y fortalecen el crecimiento tecnológico empresarial y forman relaciones de largo plazo con sus clientes. También es una empresa consultora dedicada a crear integraciones tecnológicas on-premise y cloud con la capacidad de trabajar bajo la plataforma que cada proyecto requiera, se han dedicado por mucho tiempo a conocer a profundidad cada una de las herramientas que usamos en nuestra labor para poder innovar a través de ellas brindando soluciones únicas al conectar lenguajes, plataformas, hardware, software y otros servicios web de formas que otros ni siquiera consideran posibles. Algunas situaciones que tiene esta empresa son:

* Acceso repositorio GIT después del retiro de la empresa.
* Acceso de manera remota a los equipos después del retiro de la empresa.
* Libre acceso a cualquier página de internet.
* Libre acceso a descargas de páginas de internet.
* Sabotaje en la creación de código.
* Divulgación de Información.
* Mantener credenciales después del retiro de la empresa.
* Permitir uso de memorias extraíbles en los equipos de la compañía.
* Acceso público para usuarios externos al área de Software dentro de la compañía.
* Mala gestión para generar Backup.
  + 1. Evaluación de riesgos







# LEVANTAMIENTO DE ACTIVOS – APLICACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO:01 | NOMBRE: Teams |
| DESCRIPCION: Herramienta del cual tenemos comunicación con las personas del grupo. | |
| RESPONSABLE: Empresa. | |
| TIPO: Software. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Medio | La pérdida de disponibilidad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – APLICACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO:02 | NOMBRE: GitHub |
| DESCRIPCION: Herramienta del cual se actualiza cada proyecto. | |
| RESPONSABLE: Líder Técnico. | |
| TIPO: Software. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – APLICACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO:03 | NOMBRE: [CRM.](https://www.google.com/search?rlz=1C1CHBF_esCO884CO884&sxsrf=ALeKk00JVVYrGONUjt145mdVexbbQ1X1Cg:1618351392146&q=Business+Intelligence&spell=1&sa=X&ved=2ahUKEwitx-benPzvAhWMMlkFHfXQDA0QkeECKAB6BAgBEDU) |
| DESCRIPCION: Herramienta que permite compartir y maximizar el conocimiento de un cliente dado y de esta forma entender sus necesidades y anticiparse a ellas. Por definición, el CRM recopila toda la información de las gestiones comerciales manteniendo un histórico detallado. | |
| RESPONSABLE: Líder Técnico | |
| TIPO: Software | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Medio | La pérdida de disponibilidad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – APLICACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO:04 | NOMBRE: Microsoft Office. |
| DESCRIPCION:  [Suite ofimática](https://es.wikipedia.org/wiki/Suite_ofim%C3%A1tica) que abarca el mercado completo en Internet e interrelaciona aplicaciones de escritorio, servidores y servicios para los sistemas operativos [Microsoft Windows](https://es.wikipedia.org/wiki/Microsoft_Windows), [Mac OS X](https://es.wikipedia.org/wiki/Mac_OS_X), [iOS](https://es.wikipedia.org/wiki/IOS) y [Android](https://es.wikipedia.org/wiki/Android). | |
| RESPONSABLE: Cada persona responsable. | |
| TIPO: Software. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Medio | La pérdida de disponibilidad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – APLICACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| APLICACIONES | |
| CODIGO:05 | NOMBRE: SAP |
| DESCRIPCION: Herramienta dedicada al diseño de [productos informáticos](https://es.wikipedia.org/wiki/Software) de gestión empresarial para la empresa dentro de la organización. | |
| RESPONSABLE: Líder Técnico | |
| TIPO: Software | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Medio | La pérdida de disponibilidad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – SERVICIOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO:001 | NOMBRE: Internet. |
| DESCRIPCION: Red informática de nivel mundial que utiliza la empresa para transmitir la información, el servicio de internet es Claro Empresas. | |
| RESPONSABLE: Empresa. | |
| TIPO: Hardware. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – SERVICIOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO:002 | NOMBRE: Seguridad Privada. |
| DESCRIPCION: Prestación remunerada de servicios los cuales comprenden la protección de bienes muebles o inmuebles, de las personas de la empresa. | |
| RESPONSABLE: Empresa. | |
| TIPO: Seguridad en el establecimiento. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – SERVICIOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO:003 | NOMBRE: Servicios de aseo. |
| DESCRIPCION: Servicio prestado por una empresa segundaria que prestan los servicios de aseo en la empresa. | |
| RESPONSABLE: Empresa. | |
| TIPO: Servicios Generales. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – SERVICIOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO:004 | NOMBRE: Soporte. |
| DESCRIPCION: Personas encargadas para realizar soportes de servicio puede ser en el área de tecnología, contabilidad, etc. Son empresas terciarias. | |
| RESPONSABLE: Empresa. | |
| TIPO: Mantenimiento. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – SERVICIOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| SERVICIOS | |
| CODIGO:005 | NOMBRE: Servicios generales. |
| DESCRIPCION: Servicios generales de la empresa como el agua, energía eléctrica para todas las personas que están en la empresa. | |
| RESPONSABLE: Empresa. | |
| TIPO: Software | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – EQUIPOS INFORMATICOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO:0001 | NOMBRE: Equipos de cómputo del área de tecnología. |
| DESCRIPCION: Equipos de cómputo del área de tecnología, que son de uno por persona del cual hay cinco personas en esta área. | |
| RESPONSABLE: Cada persona. | |
| UBICACIÓN: Empresa o Teletrabajo | |
| NUMERO: i7559-2512BLK | |
| TIPO: Intel Quad Core i7-6700HQ | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – EQUIPOS INFORMATICOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO:0002 | NOMBRE: Equipos informáticos en el área de Talento Humano. |
| DESCRIPCION: Equipos informáticos en el área de Talento Humano en donde hay 3 personas y de un computador por cada persona. | |
| RESPONSABLE: Cada persona. | |
| UBICACIÓN: Empresa o Teletrabajo | |
| NUMERO: E5-575G-53VG | |
| TIPO: Intel Core i5-6200U Processor | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – EQUIPOS INFORMATICOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO:0003 | NOMBRE: Equipos informáticos en el área de Vigilancia. |
| DESCRIPCION: Equipos informáticos en el área de Seguridad en donde hay 3 personas y de un computador por cada persona. | |
| RESPONSABLE: Seguridad Privada. | |
| UBICACIÓN: Empresa. | |
| NUMERO: K501UW-AB78 | |
| TIPO: Informático. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – EQUIPOS INFORMATICOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO:0004 | NOMBRE: Equipos Informáticos en el área de Contabilidad. |
| DESCRIPCION: Equipos Informáticos en el área de Contabilidad donde es asignado uno por persona, donde hay 6 personas en esta área. | |
| RESPONSABLE: Cada persona. | |
| UBICACIÓN: Empresa o Teletrabajo | |
| NUMERO: 510 80SV0058US | |
| TIPO: Intel Core i7-7500U | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – EQUIPOS INFORMATICOS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| EQUIPOS INFORMATICOS | |
| CODIGO:0005 | NOMBRE: [Equipos](https://goo.gl/UBmcqx) informáticos en el área administrativa. |
| DESCRIPCION: [Equipos](https://goo.gl/UBmcqx) informáticos del área administrativa de los cuales son el director, subdirector y jefe de cada área. | |
| RESPONSABLE: Cada persona. | |
| UBICACIÓN: Empresa o Teletrabajo | |
| NUMERO: 13.3″ IPS (2560 x 1600) | |
| TIPO: Upto 3.3GHz dual-core Intel Core i7 | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – REDES DE COMUNICACIÓN

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: 00001 | NOMBRE: WhatsApp |
| DESCRIPCION: WhatsApp es una [aplicación de mensajería instantánea](https://es.wikipedia.org/wiki/Aplicaciones_de_mensajer%C3%ADa) para [teléfonos inteligentes](https://es.wikipedia.org/wiki/Tel%C3%A9fono_inteligente), en la que se envían y reciben mensajes mediante [Internet](https://es.wikipedia.org/wiki/Internet), así como imágenes, vídeos, audios, grabaciones de audio (notas de voz), documentos, ubicaciones, contactos, gifs, stickers, así como llamadas y videollamadas con varios participantes a la vez, entre otras funciones. | |
| RESPONSABLE: Cada persona que trabaja en la empresa. | |
| UBICACIÓN: Celular de cada persona. | |
| NUMERO: 1 | |
| TIPO: Comunicaciones | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Media | La pérdida de disponibilidad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Media | La pérdida de integridad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – REDES DE COMUNICACIÓN

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: 00002 | NOMBRE: Teams |
| DESCRIPCION: Microsoft Teams es una plataforma de comunicación empresarial que reúne las mejores capacidades de Office. Teams se basa en la comunicación y colaboración basadas en chat. | |
| RESPONSABLE: Cada persona que tenga acceso o algún link para entrar a esta plataforma. | |
| UBICACIÓN: Celular o computador que tenga instalado esta plataforma. | |
| NUMERO: 2 | |
| TIPO: Comunicaciones | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alta | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alta | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – REDES DE COMUNICACIÓN

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: 00003 | NOMBRE: Meet |
| DESCRIPCION: Google Meet es la solución de Videoconferencia integrada en la plataforma G Suite. Utiliza tu Cuenta personal o tu Cuenta alumno para crear salas de videoconferencia de hasta 250 participantes, en la que podrás proyectar tu pantalla o compartir una presentación. | |
| RESPONSABLE: Cada persona que tenga acceso o algún link para entrar a esta plataforma. | |
| UBICACIÓN: Celular o computador que tenga instalado esta plataforma. | |
| NUMERO: 3 | |
| TIPO: Comunicaciones | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alta | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alta | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – REDES DE COMUNICACIÓN

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: 00004 | NOMBRE: Outlook |
| DESCRIPCION: Outlook es un programa que funciona bajo la plataforma de Windows y ha sido desarrollado por la compañía Microsoft para dar soporte a gente que necesitaba un gestor de correo electrónico. La función de este programa es recibir y mandar correos electrónicos, así como la de almacenar los mensajes recibidos y enviados. | |
| RESPONSABLE: Cada persona de la empresa que tenga acceso a esta plataforma. | |
| UBICACIÓN: Celular o computador que pueda entrar a la página de Outlook. | |
| NUMERO: 4 | |
| TIPO: Comunicaciones | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alta | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – REDES DE COMUNICACIÓN

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| REDES DE COMUNICACIÓN | |
| CODIGO: 00005 | NOMBRE: Gmail |
| DESCRIPCION: Gmail o Google mail es un servicio de correo electrónico gratuito proporcionado por el motor de búsqueda Google. ... Con Gmail, los mensajes de correo electrónico se pueden enviar y recibir a través de una interfaz de navegador en un equipo doméstico. También se puede utilizar con smartphones (iOS y Android) o tabletas. | |
| RESPONSABLE: Cada persona de la empresa que tenga acceso a esta plataforma. | |
| UBICACIÓN: Celular o computador que pueda entrar a la página de Gmail. | |
| NUMERO: 5 | |
| TIPO: Comunicaciones | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Media | La pérdida de disponibilidad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Media | La pérdida de integridad del activo afecta la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

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

# LEVANTAMIENTO DE ACTIVOS – INSTALACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO:000001 | NOMBRE: Inventarios. |
| DESCRIPCION: Es la relación detallada, ordenada y valorada de los elementos que componen el patrimonio de una empresa o persona en un momento determinado, detallado porque se especifican las características de cada uno de los elementos que integran el patrimonio. | |
| RESPONSABLE: Area de Contabilidad. | |
| UBICACIÓN: El lugar donde este ubicada la empresa. | |
| NUMERO: 1 | |
| TIPO: Instalaciones. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – INSTALACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO:000002 | NOMBRE: Archivo. |
| DESCRIPCION: Es de vital importancia, ya que, como su propio nombre indica, sirve para gestionar, clasificar y ordenar un conjunto de documentos que son necesarios conservar en su base de datos. | |
| RESPONSABLE: Archivista. | |
| UBICACIÓN: El lugar donde este ubicada la empresa. | |
| NUMERO: 2 | |
| TIPO: Instalaciones. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – INSTALACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO:000003 | NOMBRE: **Cámaras de seguridad.** |
| DESCRIPCION: Son extremadamente útiles ya que permiten monitorear las actividades de las personas que visitan su hogar y oficina, así como los eventos. Tenemos un registro de lo que sucede. Recopila pruebas de los posibles delitos – robos que se practican en la vivienda. | |
| RESPONSABLE: Seguridad privada de la empresa. | |
| UBICACIÓN: Software. | |
| NUMERO: 3 | |
| TIPO: Instalaciones. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – INSTALACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO:000004 | NOMBRE: Servidor principal. |
| DESCRIPCION: Servidor principal donde se almacena toda la información de la empresa como lo puede ser de cada persona, movimientos de información, de inventarios, etc. | |
| RESPONSABLE: Tecnología. | |
| UBICACIÓN: Datacenter. | |
| NUMERO: 4 | |
| TIPO: Instalaciones. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – INSTALACIONES

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
|  | |
| INSTALACIONES | |
| CODIGO:000005 | NOMBRE: Torniquete de ingreso. |
| DESCRIPCION: Es el control que se implementan para tener el control de todo el personal que transita en un espacio público o privado, asegurando el paso de personas que cuentan con un libre tránsito y restringiendo el paso de personas no autorizadas en áreas en la empresa. | |
| RESPONSABLE: Cada persona que tiene el carnet de acceso. | |
| UBICACIÓN: En el lugar donde está ubicada la empresa | |
| NUMERO: 5 | |
| TIPO: Instalaciones. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

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

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – PERSONAS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO:0000001 | NOMBRE: Jefe de proyecto. |
| DESCRIPCION:  Es el encargado de realizar el análisis de los requerimientos del cliente. | |
| NUMERO:1 | |
| TIPO: Personas. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – PERSONAS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO:0000002 | NOMBRE: Líder Técnico. |
| DESCRIPCION:  Es el programador líder, debe ser alguien senior, con capacidad organizativa. | |
| NUMERO:2 | |
| TIPO: Personas. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – PERSONAS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO:0000003 | NOMBRE: Desarrollador. |
| DESCRIPCION:  Es un arquitecto de software, al igual que un arquitecto «tradicional» hace con un edificio, se encargan de que la aplicación o web funcione correctamente, que sea segura, que soporte el paso del tiempo, que sea fácilmente modificable y adaptable. | |
| NUMERO:3 | |
| TIPO: Personas. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – PERSONAS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO:0000004 | NOMBRE: Líder de calidad |
| DESCRIPCION:  El líder de la calidad: como gerente, sabe que es responsable del sistema de gestión de calidad y ha implementado una política integral con objetivos detallados. ... Un liderazgo fuerte es esencial para promover la calidad dentro de la organización y, como resultado, mejorar la satisfacción del cliente. | |
| NUMERO:4 | |
| TIPO: Personas. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Muy Alto | La pérdida de disponibilidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Muy Alto | La pérdida de integridad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Muy Alto | La pérdida de confidencialidad del activo afecta totalmente la operación de los procesos de la organización, las personas y el flujo de la información. |

FIRMA DE ACEPTACION

# LEVANTAMIENTO DE ACTIVOS – PERSONAS

Nombre: Empresa

Departamento:

|  |  |
| --- | --- |
| PERSONAS | |
| CODIGO:0000005 | NOMBRE: Director. |
| DESCRIPCION:  Es quien supervisa a todos los departamentos para orientar a los empleados en sus tareas. Para eso, debe tener en cuenta las decisiones tomadas por la junta directiva. | |
| NUMERO:5 | |
| TIPO: Personas. | |

|  |  |  |
| --- | --- | --- |
| VALORACION | VALOR | JUSTIFICACION |
| DISPONIBILIDAD | Alto | La pérdida de disponibilidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| INTEGRIDAD | Alto | La pérdida de integridad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |
| CONFIDENCIALIDAD | Alto | La pérdida de confidencialidad del activo afecta considerablemente la operación de los procesos de la organización, las personas y el flujo de la información. |

FIRMA DE ACEPTACION

**4.** Identificación de amenazas y vulnerabilidades

**Vulnerabilidades:**

* Tener acceso al repositorio Git de la empresa después del retiro.
* Poder acceder a los equipos de la empresa después del retiro.
* Entregar Información sobre desarrollos a terceros.
* Poder acceder a cualquier elemento de la empresa después del retiro.
* Generar un mal Backup.

Se logro identificar estas vulnerabilidades evaluando la cantidad de peligro que causa cada una de ellas, teniendo en cuenta que esto se podría llevar en un tiempo a largo plazo. Ya que permitirán ataques hacia la empresa o los productos afectados en ese momento, limitando gubernamental las tecnologías de seguridad, pese a que representan una problemático frente a la seguridad de los datos de la compañía no se consideran amenazas debido a que relativamente son sencillos de controlar y funcionan más como puentes para verdaderas amenazas.

**Amenazas:**

* Poder bajar un virus a través de una página web.
* Poder bajar un virus a través de un archivo.
* Afectar a desarrolladores y a la misma empresa por copia de un desarrollo.
* Poseer un virus a través de memorias extraíbles.
* Filtrar información a personas que no sean afectadas o no les corresponde tener esta información.

Se logro identificar estas amenazas ya que son persistentes y avanzadas con una forma parasitaria de ataque que puede ocasionar cualquier persona de manera intencional o no intencional en los sistemas y de esta manera establecer un punto de apoyo en la infraestructura de la empresa a partir de las cuales contrabandean datos y propiedad intelectual.

# REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Hora de notificación: 12:52

Fecha de notificación: 05-01-2021

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: Daniel Córdoba Marín | | |
| Sede.: Principal | | Área / Dependencia: Tecnología |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: 15-01-2021 | | Hora en que observó el incidente: 12:01 | |
| 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 |
|  |  |
| **x** | 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: La persona Camila Vera identificada con cedula de ciudadanía No. 1.109.456.785, se visualiza que mediante una llamada de Teams está compartiendo la pantalla y comparte información a terceros y se hace su respectivo proceso a la persona que está cometiendo este delito dentro de la empresa.  **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 detecto ya que en la empresa se hace seguimiento semanalmente a las personas. |
| El incidente aún está en progreso: [ ] SI [X ] NO |
| Tiempo estimado de duración del incidente: 1 HORA |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: La persona de recursos humanos, seguridad privada y el ente encargado de hacer este tipo de movimientos en la empresa. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: Información Crítica. | | | | |
| Localización física: Empresa | | | | |
| Describa brevemente la información contenida en el sistema / computador: Información sobre desarrollos y temas privados de la compañía. | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? | X | SI |  | NO |
| ¿El recurso afectado tiene conexión con la red? |  | SI | X | 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: Karen Vargas  Datos de contacto:  3042568795 |
| Apellido y nombres: Luis Carvajal  Datos de contacto:  3145647896 |

# REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Hora de notificación: 18:21

Fecha de notificación: 15-03-2021

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

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: 30-02-2021 | | Hora en que observó el incidente: 15:01 | |
| 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. | **x** | 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: La persona Stiven Garrido eliminando información, también aplicativos que a la vez esta misma puede ser valiosa en cualquier oportunidad. Se hace su proceso correspondiente ya que él no tenía ninguna autorización para realizar este tipo de solicitudes.  **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 detecto haciendo un proceso del cual no tiene ningún tipo de autorización. |
| El incidente aún está en progreso: [ X ] SI [ ] NO |
| Tiempo estimado de duración del incidente: 45 MINUTOS |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: La persona de recursos humanos, seguridad privada y su jefe inmediato. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: Información Crítica. | | | | |
| Localización física: Empresa | | | | |
| Describa brevemente la información contenida en el sistema / computador: Información sobre desarrollos y temas privados de la compañía. | | | | |
| ¿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: Daniela Cárdenas  Datos de contacto:  3021204564 |
| Apellido y nombres: Armando Casas  Datos de contacto:  3214569874 |

# REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Hora de notificación: 18:30

Fecha de notificación: 12-12-2020

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: Yulieth García | | |
| Sede.: Chapinero | | Área / Dependencia: Seguridad Privada de la empresa |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: 30-02-2021 | | Hora en que observó el incidente: 15:01 | |
| 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. | **x** | Robo o pérdida de un recurso informático. |
|  |  |
|  | Acceso o intento de acceso no autorizado a un sistema informático. | **X** | Otro no contemplado. Describa: Ingreso de memoria USB |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente: La persona Esteban Quito se descubre que está ingresando memorias de la compañía a computadores de la empresa, se verifica esta información mediante una cámara de seguridad. Se hace su respectivo proceso y a la vez el despido de esta persona.  **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: Robo de Información y incumpliendo las normas de la empresa. |
| El incidente aún está en progreso: [ ] SI [X ] NO |
| Tiempo estimado de duración del incidente: 45 MINUTOS |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: La persona de recursos humanos, seguridad privada y su jefe inmediato. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: Computador Windows 7 e información confidencial de la compañía. | | | | |
| Localización física: Empresa | | | | |
| Describa brevemente la información contenida en el sistema / computador: Información sobre desarrollos y temas privados de la compañía. | | | | |
| ¿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? |  | SI | x | 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: Milena Cervantes  Datos de contacto:  3154789655 |
| Apellido y nombres: Carlos Arredondo  Datos de contacto:  3214569874 |

# REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Hora de notificación: 08:30

Fecha de notificación: 01-12-2020

|  |  |  |
| --- | --- | --- |
| **DATOS DE LA PERSONA QUE NOTIFICA** | | |
| Apellido y Nombres: Tulio Casas | | |
| Sede.: Principal | | Área / Dependencia: Seguridad Privada. |
| Correo electrónico: | |  |
| Teléfono: | Interno: | Teléfono particular: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: 10-11-2020 | | Hora en que observó el incidente: 10:59 | |
| 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. | 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: Ingreso de memorias USB. |
|  |  |

|  |
| --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** |
| Describa el incidente: La persona María Ramos se descubre que ingresando una memoria USB al computador del cual no se puede hacer en la empresa y consecuente de este, la memoria USB contenía virus. Se hace el respectivo proceso y despido de la persona.  **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 virus que ingreso al computador es MyDoom. |
| El incidente aún está en progreso: [ ] SI [ X] NO |
| Tiempo estimado de duración del incidente: 10MINUTOS |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: La persona de recursos humanos, seguridad privada y su jefe inmediato. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: Computador y además que esta haciendo daño a los demás procesadores ya que el computador que asedio es uno de los principales por la compañía. | | | | |
| Localización física: Empresa | | | | |
| Describa brevemente la información contenida en el sistema / computador: Información sobre desarrollos y temas privados de la compañía. | | | | |
| ¿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: Karen Vargas  Datos de contacto:  3195789654 |
| Apellido y nombres: Pedro Vela  Datos de contacto:  3168978457 |

# REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Hora de notificación: 17:01

Fecha de notificación: 01-10-2020

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

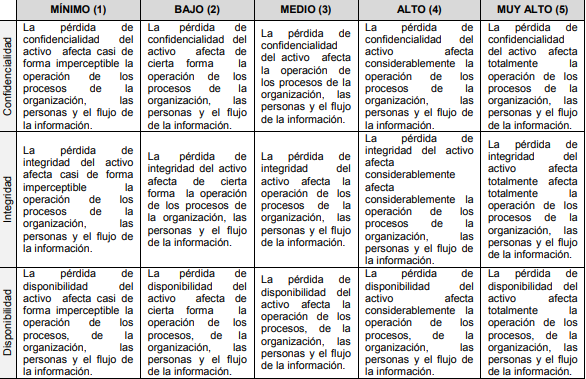
|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | |
| Fecha en que observó el incidente: 18-09-2020 | | Hora en que observó el incidente: 13:12 | |
| Marque con una cruz todas las opciones que considere aplicables. | | | |
|  | Uso indebido de información crítica. |  | Ingeniería social, fraude o phishing. |
| **x** | 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: La persona Gabriela Mora se visualiza entrando a paginas de internet donde no se debe acceder y mas que esto, le hace entrar un virus al computador. Se hace el debido proceso de seguimiento y se despide esta persona.  **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: Virus que ataca es SoBig en la red del computador. |
| El incidente aún está en progreso: [ ] SI [ X] NO |
| Tiempo estimado de duración del incidente: 2 HORAS |
| Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente: La persona de recursos humanos, seguridad privada y su jefe inmediato. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **INFORMACIÓN SOBRE EL RECURSO AFECTADO** | | | | |
| Sistema, computadora o red afectada: El computador y a toda la red del computador puede tener acceso. | | | | |
| Localización física: Empresa | | | | |
| Describa brevemente la información contenida en el sistema / computador: Información sobre desarrollos y temas privados de la compañía. | | | | |
| ¿Existe copia de respaldo de los datos o software afectado? |  | SI | X | 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: Daniel Miranda  Datos de contacto:  3186578965 |
| Apellido y nombres: Miguel González  Datos de contacto:  3124568794 |



**Reporte Vulnerabilidades Ip**

# 

# 

# 

# 

# 

**Conclusiones**

Se identifica que en los primeros cuatro casos de las paginas, son tipos de pruebas ejecutados por las paginas los puertos se encuentran cerrados lo cual confirma que tienen cierta seguridad, sin embargo, se recomienda mantener unas buenas métricas de seguridad para evitar problemas a futuro. En el último caso se identificó que tenía una vulnerabilidad en el puerto 80 el cual permitía que el virus troyano Bayrob pudiera acceder a través de la ip y pudiese infectar el sistema por esta razón se recomienda realizar el debido análisis de seguridad informática para determinar si se puede bloquear esta ip y evitar problemas a futuro.