**DOCUMENTO DE SEGURIDAD DE LA INFORMACION DE LA JUNTA ESTATAL DE CAMINOS**

Version: 1.01

Fecha última versión: 17 de diciembre de 2018

# CONTENIDO

ANTECEDENTES Y JUSTIFICACIÓN

INVENTARIO DE DATOS PERSONALES

FUNCIONES Y OBLIGACIONES

ANALISIS DE RIESGOS

ANALISIS DE BRECHA

PLAN DE TRABAJO

MECANISMOS DE MONITOREO

PROGRAMA DE CAPACITACION

# ANTECEDENTES Y JUSTIFICACIÓN

La Junta Estatal de Caminos del Gobierno del Estado de Tabasco cumple con las leyes y normatividad vigente en materia de acceso y tratamiento de los Datos Personales. Por lo tanto se fundamenta y apoya en el cumplimiento a dichas disposiciones contenidas en los artículos 9 fracción VI; 12, 45 fracciones X, XI y XIII, 124 y 128 primer párrafo de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Tabasco, así como los artículos 3 fracciones I, III, VIII, IX, VIII, IX, 14, 16, 72, 73, 96 fracciones I, III, VIII, XVI, XXIII, y XXVII todos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de tabasco, articulo 23 de Lineamientos de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tabasco, de igual forma los artículos 4 bis fracción III y IV de la Constitución Política del Estado Libre y Soberano de Tabasco, artículos 6 apartado A fracciones I, II, III y artículo 16 segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, Reglamento Interior de la Junta Estatal de Caminos, así como toda la normatividad aplicable.

Dichas disposiciones reconocen que la privacidad y la seguridad de la información personal es un derecho humano importante, por lo que está comprometida a resguardarla, bajo criterios de seguridad legal, tecnológicos y administrativos.

Este Documento de Seguridad tiene como propósito guiar los esfuerzos de la JEC en la protección de datos personales.

# INVENTARIO DE DATOS PERSONALES

Los sistemas de datos personales que tiene la Junta Estatal de Caminos se listan a continuación:

1. Sistema de información de visitantes
2. Sistema de información de contratistas de obra pública
3. Sistema de información del personal

En cada sistema se detalla la información solicitada y el tratamiento que se hará con la información en cada caso. A continuación se listan los datos que se incluyen en cada sistema de información de datos personales.

# FUNCIONES Y OBLIGACIONES DE TRATAMIENTO DE DATOS PERSONALES

## CUADRO DE FUNCIONES Y OBLIGACIONES DE SEGURIDAD DE INFORMACIÓN

|  |  |  |
| --- | --- | --- |
| **CARGO** | **FUNCIONES** | **OBLIGACIONES** |
| Director General | Instruir la elaboración del plan de seguridad de información de la JEC | Verificar que se elabore el plan en los tiempos establecidos.  Aprobar el plan de seguridad de la información. |
| Directora de Administración | Coordinar la elaboración del plan de seguridad de información de la JEC | Elaborar políticas de seguridad de la información.  Dar seguimiento al plan de seguridad de la información. |
| Titular de la Unidad de Asuntos Jurídicos y Transparencia | Coordinar los trabajos de tratamiento y protección de datos personales | Elaborar políticas de protección de datos personales.  Dar seguimiento al plan de seguridad de la información. |
| Comité de Transparencia | Evaluar los incidentes relacionados a los datos personales procesados por la JEC | Recibir los reportes cuando ocurran vulneraciones a los datos personales y elaborar el aviso a las instancias correspondientes |
| Unidad de Seguimiento y Evaluación | Elaborar el programa de seguimiento al plan de seguridad de la información. | Dar seguimiento al plan de seguridad de la información. |
| Departamento de Tecnologías de la Información y Comunicaciones | Integrar el plan de seguridad de la información. | Coordinarse con la Dirección de Administración y la Unidad de Asuntos Jurídicos y Transparencia para la elaboración de las políticas de seguridad de la información.  Elaboración del análisis de riesgos de seguridad de la información.  Elaborar el análisis de brecha.  Elaborar el plan de seguridad de la información.  Monitorear y presentar informes de incidentes y problemas en la seguridad de la información. |

# ANALISIS DE RIESGOS

## Identificación de riesgos

Los tipos de riesgos considerados son

|  |  |
| --- | --- |
| **Tipo de Riesgo** | **Riesgo** |
| De acceso físico | Acceso no autorizado a instalaciones |
|  | Acceso no autorizado al cuarto de comunicaciones |
| De acceso de equipos | Acceso no autorizado a la computadora personal |
|  | Acceso no autorizado a los servidores |
|  | Acceso no autorizado a los equipos de red |
| De acceso a la información | Acceso no autorizado a archivos |
| De pérdida de información | Pérdida de información por infección de virus, malware o ransomware. |
|  | Pérdida de información por uso de programas vpn no autorizados |
|  | Perdida de información por problemas en el hardware o sistema operativo |
|  |  |

## Evaluación de riesgos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tipo de Riesgo** | **Riesgo** | **Impacto** | **Probabilidad** | **Se atiende** |
| De acceso físico | Acceso no autorizado a instalaciones | BAJO | BAJA | SI |
|  | Acceso no autorizado al cuarto de comunicaciones | ALTO | BAJO | SI |
| De acceso de equipos | Acceso no autorizado a la computadora personal | BAJO | ALTO | SI |
|  | Acceso no autorizado a los servidores | ALTO | BAJA | SI |
|  | Acceso no autorizado a los equipos de red | ALTO | BAJA | SI |
| De acceso a la información | Acceso no autorizado a archivos | ALTO | ALTO | SI |
| De pérdida de información | Pérdida de información por infección de virus, malware o ransomware. | ALTO | ALTO | SI |
|  | Pérdida de información por uso de programas vpn no autorizados | BAJO | ALTA | SI |
|  | Perdida de información por problemas en el hardware o sistema operativo | ALTO | ALTA | SI |

## Respuesta a riesgos

|  |  |  |
| --- | --- | --- |
| **Tipo de Riesgo** | **Riesgo** | **Acción recomendada** |
| De acceso físico | Acceso no autorizado a instalaciones | Hacer uso de personal de control de acceso.  Usar una bitácora de entrada. |
|  | Acceso no autorizado al cuarto de comunicaciones | Utilizar cerraduras para restringir el acceso.  Llevar un control de los accesos del cuarto de comunicaciones. |
| De acceso de equipos | Acceso no autorizado a la computadora personal | Cada Usuario es responsable del acceso a su cuenta y a sus computadoras. |
|  | Acceso no autorizado a los servidores | Se manejan cuentas y contraseñas controladas para el personal de TI |
|  | Acceso no autorizado a los equipos de red | Se manejan contraseñas en los equipos de res controladas para el personal de TI  Se restringe el acceso a los equipos desde internet con el firewall. |
| De acceso a la información | Acceso no autorizado a archivos | Establecer permisos a información de cada área con cuentas y contraseñas de Directorio Activo previa autorización de los Directores involucrados. |
| De pérdida de información | Pérdida de información por infección de virus, malware o ransomware. | Uso de programas de antivirus, antimalware y antiransomware.  Uso de antivirus de solución de firewall. |
|  | Pérdida de información por uso de programas vpn no autorizados | Configurar las políticas de restricción de aplicaciones y páginas web |
|  | Perdida de información por problemas en el hardware o sistema operativo | Elaborar un plan de respaldos de información  Elaborar un reporte semanal del proceso de respaldos. |

Tabla de respuesta a riesgos

# ANALISIS DE BRECHA

|  |  |  |  |
| --- | --- | --- | --- |
| **RIESGOS Y VULNERABILIDADES** | **ACCION** | **SE ESTA REALIZANDO** | **SE PROYECTA REALIZAR** |
|  |  |  |  |
| **RIESGOS** |  |  |  |
| Acceso no autorizado a instalaciones | Hacer uso de personal de control de acceso.  Usar una bitácora de entrada. | X |  |
| Acceso no autorizado al cuarto de comunicaciones | Utilizar cerraduras para restringir el acceso.  Llevar un control de los accesos del cuarto de comunicaciones. | X |  |
| Acceso no autorizado a la computadora personal | Cada Usuario es responsable del acceso a su cuenta y a sus computadoras. | X |  |
| Acceso no autorizado a los servidores | Se manejan cuentas y contraseñas controladas para el personal de TI | X |  |
| Acceso no autorizado a los equipos de red | Se manejan contraseñas en los equipos de res controladas para el personal de TI  Se restringe el acceso a los equipos desde internet con el firewall. | X |  |
| Acceso no autorizado a archivos | Establecer permisos a información de cada área con cuentas y contraseñas de Directorio Activo previa autorización de los Directores involucrados. | X |  |
| Pérdida de información por infección de virus, malware o ransomware. | Uso de programas de antivirus, antimalware y antiransomware.  Uso de antivirus de solución de firewall. |  | X |
| Pérdida de información por uso de programas vpn no autorizados | Configurar las políticas de restricción de aplicaciones y páginas web |  | X |
| Perdida de información por problemas en el hardware o sistema operativo | Elaborar un plan de respaldos de información  Elaborar un reporte semanal del proceso de respaldos. | X |  |
|  |  |  |  |
| **VULNERABILIDADES** |  |  |  |
| Licencia de Firewall  (Antivirus, Supervisión de conexiones seguras, Detección de intrusos, filtrado de contenido) | Renovar licencias. Vencen el 3 de noviembre de 2018 |  | X |
| Licencia de sistemas operativos de escritorio | Solicitar licencias |  | X |
| Licencia de sistemas operativos de servidor | Solicitar licencias |  | X |
| Licencia de antivirus y antiransomware | Solicitar licencias |  | X |
| Baja cultura de seguridad de información del personal de la JEC | Programa de capacitación |  | X |

# PLAN DE TRABAJO

|  |  |
| --- | --- |
| **ACTIVIDAD** | **FECHA** |
|  |  |
| Elaborar la relación actualizada de equipos de cómputo de la JEC | 30 de noviembre de 2018 |
| Elaborar las políticas de Seguridad de la Información de la JEC | 30 de noviembre de 2018 |
| Ejecutar las políticas de Seguridad de la Información | 30 de noviembre de 2018 |
| Diseñar la configuración de equipos para el cumplimiento de la política de seguridad | 30 de noviembre de 2018 |
| Elaborar el programa de Capacitación en Seguridad de la Información | 30 de noviembre de 2018 |
| Recopilar los incidentes de Seguridad con los Mecanismos de Monitoreo. | Acción Permanente |
| Evaluar la necesidad de cambios en el documento de Seguridad de Información | Cuando se presente un cambio |
| Elaborar los cambios al documento cuando estos procedan | Cuando se presente un cambio |

## MECANISMOS DE MONITOREO

|  |  |
| --- | --- |
| **Puntos a monitorear** | **Formas de monitoreo** |
|  |  |
| Presencia de Virus y Ransomware | Revisar la vigencia de las licencias del software de punto final (antivirus y antiransomware) |
| Accesos al cuarto de comunicaciones | Controlar las copias de las llaves y la bitácora de acceso |
| Accesos a Servidores críticos | Revisar los archivos Log de los Servidores reportar incidencias |
| Acceso a carpetas compartidas y aplicaciones | Documentar accesos a los recursos aprobados por el Área Correspondiente. |
| Acceso a la red de datos de la JEC | Revisar los reportes del Firewall y reportar incidencias. |

# PROGRAMA DE CAPACITACION

Capacitación: Protección de datos Personales y Seguridad de la Información

Dirigido a: Personal de las diferentes Unidades Administrativas de la JEC

Capacidad por sesión: 15 personas

Duración: 1 hora

Periodo de la impartición del curso: Del 14 al 31 de enero de 2019

Fecha de las sesiones: Por confirmarse

# ANEXOS

**BITACORA DE INCIDENCIAS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **INCIDENCIA** | **FECHA Y HORA** | **PERSONA QUE REPORTA** | **PERSONA QUE RECIBE LA NOTIFICACION** | **EFECTOS DE LA INCIDENCIA** | **ACCIONES IMPLEMENTADAS** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |