PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – PETI 2020

(Original firmado por)

ARQUITECTO JUAN EDUARDO QUINTERO LUNA
Gerente Empresas Públicas de Cundinamarca SA ESP

Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co

INTRODUCCIÓN

La seguridad de la Información en las entidades tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Es por esto que EPC SA ESP, dentro de su política de gestión del riesgo, vincula acciones para el control de la seguridad de la información y las actividades de valoración de actos inseguros bajo el objetivo de mantener la información de la empresa de manera mucho mas confiable, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, gestión, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.

Integridad: Propiedad que la información se mantenga exacta y completa.

Disponibilidad: propiedad que la información sea accesible y utilizable en el momento que se requiera.

OBJETIVO

Generar acciones frente a la gestión del riesgo bajo enfoque sistemático para una gestión que fortalezca la seguridad de la información en Empresas Públicas de Cundinamarca EPC SA ESP.

ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la EPC SA ESP que administre sistemas de información a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, tomando como base la guía emitida por el DAFP.

Metodología de Análisis de Riesgos:

1- Identificar los activos de Información de cada proceso
2- Identificación de los responsables y dueños de la información (dependencia que produce el activo)
3- Identificar: Vulnerabilidades, Amenazas o Causas, Posibles consecuencias, Riesgo (Entrevistas, Observación directa, etc.)
4- Determinar la probabilidad de ocurrencia para cada riesgo.
5- Determinar nivel de valoración del impacto para cada riesgo materializado.
6- Determinar el nivel de riesgo basados en la probabilidad de ocurrencia y la valoración del Impacto.

Definiciones:

Factor de Riesgo:

Aquellos que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta.
Procesos	Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.
Factores Externos	Condiciones generadas por agentes externos, las cuales no son controlables por la administración y que afectan de manera directa o indirecta el proceso.

Tipos de Activos:

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes o vitales para la Administración de la Entidad:** Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba.
Hardware / Infraestructura	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.

TIPO DE ACTIVOS	DESCRIPCIÓN
Software / Aplicaciones Informáticas	**Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.** Ejemplo: Desarrollo Inhouse, Desarrollo Subcontratado, Estándar, Navegador, Servidor de Presentación (www), Servidor de Aplicaciones (app), Cliente de Correo Electrónico, Servidor de Correo Electrónico, Servidor de Ficheros (file), Sistemas de Gestión de Bases de Datos (dbms), Monitor Transaccional, Ofimática, Antivirus, Sistema Operativo (OS), Servidor de Terminales, Sistema de Backup o Respaldo, Gestor de Máquinas Virtuales.
Servicios	**Funciones que permiten suplir una necesidad de los usuarios (del servicio).** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública).
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
Soportes de Información	**Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (rdsi).
Claves Criptográficas	**Esenciales para garantizar el funcionamiento de los mecanismos criptográficos.**

Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co

TIPO DE ACTIVOS	DESCRIPCIÓN
	Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

PROCEDIMIENTO DE DILIGENCIAMIENTO:

Se trata de una hoja Excel. Las primeras cuatro columnas ya están diligenciadas.
La cuarta es la descripción del activo al que se le va a evaluar el riesgo-

REGISTRO DE ACTIVOS DE INFORMACIÓN								VALORACIÓN DEL ACTIVO				ANALISIS DE RIESGOS RIESGO DE SEGURIDAD Y PRIVACIDAD				VALORACION DEL RIESGO INHERENTE DE SEGURIDAD Y			CONTROLES EXISTENTES
PROPIETARIO / RESPONSABLE	PROCESO AL QUE PERTENECE	ID	NOMBRE	TIPO (E/F)	DESCRIPCIÓN DEL ACTIVO	MEDIO DE ALMACENAMIENTO	DISPONIBLE PARA CONSULTA	TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	FACTOR DE RIESGO	VULNERABILIDAD / DEBILIDAD	CAUSA / AMENAZA	Consecuencia	PROBABILIDAD	IMPACTO	TIPIFICACIÓN DEL RIESGO	Descripción de la Actividad o Control Existente
Maribel Rojas	Gestión de Talento Humano	1	Actas	Ambos	Documentos	Discos Duros/sub o/Físico	SI	Documentos	3	0	1	Tecnología	Falta de conocimiento el personal	Mala manipulación	Pérdida de tiempo; daño de información	3	3	MODERADO	Capacitación una vez al año

COLUMNA E:

TIPO (E/F): Describe la forma en que está almacenado el activo de información. Es posible diligenciar esta columna con una de las siguientes tres opciones:

- Electrónico
- Físico
- Ambos

COLUMNA G:

Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co

MEDIO DE ALMACENAMIENTO: Es con el fin de determinar el lugar donde se está almacenando el activo de información objeto de esta evaluación. Puede ser Discos, CDs, la Nube, En Físico, o una combinación de ellas.

VALORACION DEL ACTIVO:

VALORACIÓN DEL ACTIVO			
TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Documentos	3	0	1

Se va a realizar en las columnas I a L. Y se va a determinar en orden de importancia cuál de los pilares de la seguridad es más importante para ese activo.

Confidencialidad: Que el contenido de ese activo no sea visto sino únicamente por quien está autorizado para verlo.

Integridad: Que ese activo de información no vaya a ser modificado, sino por las personas autorizadas para tal fin.

Disponibilidad: Que el activo de información esté disponible en el momento y lugar que se necesite.

Criterios de Valoración de Activos:

Criterio	Valor
Alto	4 -5
Medio	2 – 3
Bajo	0 – 1

FACTORES DE RIESGO: Se evaluarán en las columnas N a Q, como se puede ver en la siguiente figura:

ANÁLISIS DE RIESGOS RIESGO DE SEGURIDAD Y PRIVACIDAD			
FACTOR DE RIESGO	VULNERABILIDAD / DEBILIDAD	CAUSA / AMENAZA	Consecuencia
Tecnología	Falta de conoicimiento el personal	Mala manipulación	Pérdida de tiempo; daño de información

Y los factores de riesgo posibles sobre el activo que se está evaluando pueden ser:

-Personas
-Procesos
-Tecnologías
-Infraestructura
-Factores Externos

Los factores de riesgo corresponden a aquellos agentes que actúan como Disparador de la amenaza

Los factores de riesgo se determinan a partir de:

1. Las vulnerabilidades o debilidades más importantes que puedan llegar a afectar el activo de información que se está evaluando. Ejemplo: Falta de conocimiento del personal.

2. La causa /Amenaza que podría llegar a explotar esa vulnerabilidad. Por ejemplo, la mala manipulación del activo de información.

3. La consecuencia de la explotación de esa vulnerabilidad puede ser en nuestro ejemplo la pérdida de tiempo y el daño en la información. Dentro de las posibles consecuencias podemos enumerar:

-Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
-Salud y seguridad
- Costo financiero

Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co

- Imagen, reputación y buen nombre.

VALORACION DEL RIESGO INHERENTE:

Se va a evaluar en las columnas S a V, como se muestra en la siguiente figura;

VALORACIÓN DEL RIESGO INHERENTE DE SEGURIDAD Y PRIVACIDAD DE LA		
PROBABILIDAD	IMPACTO	TIPIFICACIÓN DEL RIESGO
3	3	MODERADO

Niveles de valoración de **Probabilidad de Ocurrencia**:

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
1	**Rara Vez**	Puede que no se haya presentado u ocurrir solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años
2	**Improbable**	Pudo ocurrir en algún momento, es poco común o frecuente	Al menos una vez en los últimos 5 años
3	**Posible**	Puede ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	**Probable**	Ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año
5	**Casi Seguro**	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año

Niveles de valoración del **Impacto**:

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
1	**Insignificante**	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Afecta a una actividad del proceso.

Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2	**Menor**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
3	**Moderado**	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Afecta un conjunto de datos personales o el proceso.
4	**Mayor**	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios conjuntos de datos personales o procesos de la organización.
5	**Catastrófico**	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.	Afecta toda la organización. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la organización.

TIPIFICACION DEL RIESGO:

Se puede determinar mediante la siguiente tabla:

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	**Mayor o igual a 20**	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	**Mayor o igual a 15 y menor a 20**	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.

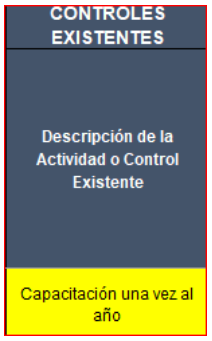
Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co

Riesgo Moderado	**Mayor o igual a 10 y menor a 15**	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
Riesgo Menor	**Mayor o igual a 5 y menor a 10**	Mitigar el riesgo mediante de medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.
Riesgo Bajo	**Menor a 5 y mayor a 0**	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.

Niveles de riesgo validos (Dimensión del riesgo)

CONTROLES EXISTENTES PARA REDUCIR EL RIESGO:

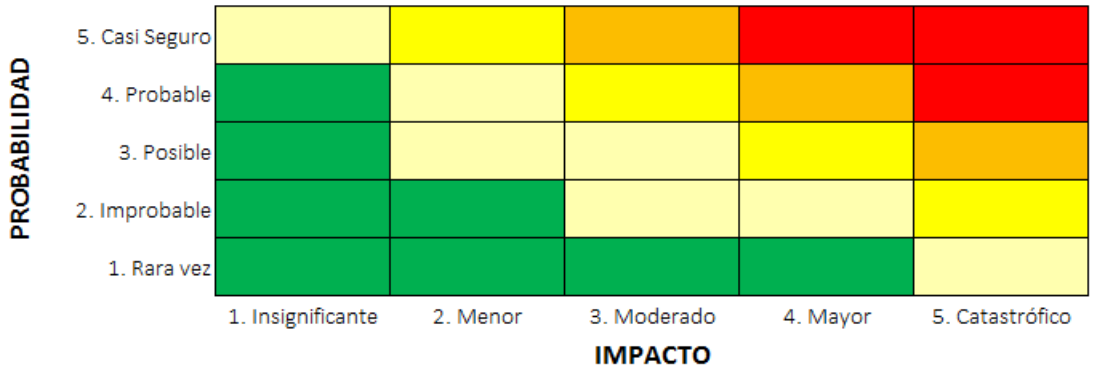
Se trata de establecer si la entidad está ejecutando algún tipo de plan para reducir el impacto del riesgo establecido, en caso de que se llegara a materializar



En el ejemplo de la figura, la actividad descrita es la realización de capacitaciones anuales.

Valoración del Riesgo: (Probabilidad x Impacto)

Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co



Acciones requeridas según el Nivel de riesgo calculado:

Zona de Riesgo Aceptable	**Asumir el Riesgo:** Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
Zona de Riesgo Tolerable	**Mitigar el Riesgo:** Riesgos que se puede permitir gestionar, que en caso de materialización la entidad se encuentra en la capacidad de asumirlo.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Importante	**Mitigar o Evitar el Riesgo:** Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
Zona de Riesgo Inaceptable	**Evitar el Riesgo:** Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos de conformidad a la gestión de la empresa, por tanto, podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

Calle 24 #51-40 Bogotá D.C.
Capital Tower-Pisos 7,10 y 11
Código Postal: 111321 – Tel: 7954480
Empresas Públicas de Cundinamarca
@EPC_SA
www.www.epc.com.co

(1) nuevos activos o modificaciones en el valor de los activos,
(2) nuevas amenazas
(3) cambios o aparición de nuevas vulnerabilidades
(4) aumento de las consecuencias o impactos,
(5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición que permitan contextualizar una toma de decisiones de manera oportuna.

CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Se definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento de la misión de EPC SA ESP.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

El presente plan tiene por objetivo comprender e implementar las acciones tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

La definición del marco de seguridad y privacidad de la información y de los sistemas de información en la empresa, define el estado actual del nivel de seguridad y privacidad y las acciones a implementar.

DIAGNÓSTICO DE SEGURIDAD Y PRIVACIDAD

Empresas Públicas de Cundinamarca EPC SA ESP, busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información, basándose en el M.S.P.I. Modelo de Seguridad y Privacidad de la Información para GEL. Para lo cual cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los riesgos, definiendo y gestionando las respectivas acciones a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo.

IMPLEMENTACIÓN

Empresas Públicas de Cundinamarca EPC SA ESP, implementa el plan de seguridad y privacidad de la información y de los sistemas de información desarrollando las estrategias de Gestión de riesgos de seguridad y privacidad de la información, buscando proteger los derechos de los usuarios y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información, para lo cual toma como base el M.S.P.I. Modelo de Seguridad y Privacidad de la Información para GEL del cual describe sus directrices en el "Plan de tratamiento de riesgos de seguridad y privacidad de la información vigencia 2020".

MONITOREO Y MEJORAMIENTO CONTINUO

El plan de seguridad y privacidad de la información, busca desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información con los que cuenta Empresas Públicas de Cundinamarca EPC SA ESP, realizando las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información, para lo cual se toma como base el M.S.P.I. Modelo de Seguridad y Privacidad de la Información para GEL

EPC SA ESP cuenta con actividades para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad, con el fin de generar los ajustes o cambios pertinentes y oportunos. De igual forma se revisa e implementa acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la información.