

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 1 de 13

INDICE

1	OBJETIVO DEL PROCEDIMIENTO.....	2
2	MOTIVO DE CAMBIO	2
3	ALCANCE	2
4	DEFINICIONES/ABREVIACIONES	2
5	DOCUMENTOS A CONSULTAR	3
6	CONDICIONES GENERALES	3
7	RESUMEN DE RESPONSABILIDADES	3
8	PROCEDIMIENTOS	3
8.1	Control Físico.....	3
8.2	Señalización de área restringida	3
8.3	Del Acceso a los servicios Informáticos.	4
8.4	De la Seguridad de Acceso a la red.	4
8.5	Seguridad en los Sistemas Informáticos para los Usuarios	6
8.6	De la Seguridad en los Puertos de Entrada (USB)	7
8.7	De la Detección de Abusos a los Sistemas Informáticos	7
8.8	De la Sanciones a los Infractores por Incumplimiento al Procedimiento	7
8.9	Del Acceso al Software de Terceros	9
8.10	De la Creación de Nuevos Usuarios	9
8.11	De la asignación de roles y transacciones en SAP	9
8.12	De la Baja de Usuarios	10
8.13	De la Pantalla de Bloqueo	10
8.14	Del Back Up. (Copia de seguridad)	10
8.15	Control y Monitoreo	10
8.16	Del Mantenimiento Preventivo.....	12
8.17	De las Capacitaciones	12
8.18	De la Contingencia	12
9	REFERENCIAS/ANEXOS	13

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 2 de 13

1. OBJETIVO DEL PROCEDIMIENTO

Garantizar el cumplimiento de los procedimientos aplicando mecanismos de seguridad y acceso a los sistemas de información e informático para preservar la integridad, disponibilidad y seguridad de la información, que obren en contra de los intereses de la empresa.

2. MOTIVO DE CAMBIO

“Cambio de documento a nuevo formato y codificación Prodac”.

3. ALCANCE

Esta política está dirigido al personal de la compañía el cual hace uso de la información y equipos de cómputo para el desempeño de sus labores en la empresa PRODAC S.A.

Los controles y gestión de seguridad se implementan para mitigar el riesgo en la Gestión de activos, redes, plataformas tecnológicas, e información.

4. DEFINICIONES/ABREVIACIONES

- **Antivirus:** Programa informático que sirve para detectar y eliminar virus y otros programas perjudiciales.
- **Área crítica:** Espacio físico en el que se identifica una alta probabilidad de ocurrencia de riesgos (o combinación de estos) que representen un impacto significativo en la seguridad de la empresa.
- **Backup:** Proceso que realiza una copia de respaldo de la información.
- **Base de Datos:** Software destinado a gestionar el almacenamiento de la información, así como el acceso al mismo.
- **Hardware:** Parte física de un ordenador o sistema informático.
- **Login:** Palabra clave de conexión al servidor de red.
- **Password:** Contraseña para uso propio de cada usuario.
- **Restauración:** Proceso por el cual se recupera la información respaldada.
- **Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
- **UPS:** Fuente de suministro eléctrico que posee una batería.
- **TI:** Tecnología de la información.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 3 de 13

5. DOCUMENTOS A CONSULTAR

No aplica

6. CONDICIONES GENERALES

No aplica

7. RESUMEN DE RESPONSABILIDADES

7.1 El Gerente de Administración y Finanzas

- ✓ Aprobar este documento,
- ✓ Asegurar el suministro de los recursos físicos y financieros para la ejecución del plan de continuidad

7.2 El Gerente de TI

- ✓ Liderar el proceso de continuidad operacional
- ✓ Activar el plan de ciberseguridad

7.3 Equipo de Soporte e Infraestructura:

- ✓ Identificar las amenazas en la seguridad de sistemas de información
- ✓ Evaluar el impacto de los riesgos en cada uno de los servicios
- ✓ Establecer y actualizar el plan de recuperación
- ✓ Planificar, realizar y evaluar los simulacros al plan de continuidad

8. PROCEDIMIENTOS

8.1 Control Físico

8.1.1 La empresa cuenta con la infraestructura tecnológica y el equipamiento necesario para realizar todas sus labores dentro de un proceso seguro para la información sensible.

8.2 Señalización de área restringida

8.2.1 Se cuenta con señalización de áreas críticas y son:

8.2.1.1 Cartel de Acceso No Autorizado para la Sala de Servidores.

8.2.1.2 Cartel de Acceso No Autorizado al almacén de TI.

8.2.1.3 La sala de servidores cuenta con detector de humo y aire acondicionado.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 4 de 13

8.3 Del Acceso a los servicios Informáticos.

8.3.1 La Seguridad Física de las PC, laptops, como los servidores y equipos móviles, es responsabilidad directa del Gerente de TI y es supervisada por el Gerente de Administración y Finanzas.

8.3.2 El acceso al sistema operativo de los servidores **es** administrado por el administrador de Redes y comunicaciones mediante una clave única que es compartida mediante la plataforma Keeper Security.

8.3.3 Contamos con dos niveles de acceso: Administrador y Usuarios.

Solo el nivel de administrador tiene acceso a cambios críticos en la configuración de los equipos. Esta clave es manejada únicamente por el Gerente de Sistemas y el Administrador de Redes e Infraestructura mediante la plataforma Keeper Security.

8.3.4 El acceso al Data Center se realiza mediante código maestro o biométrico.

8.4 De la Seguridad de Acceso a la red.

El Administrador de Infraestructura de Sistemas administra las claves de acceso de Windows, correo electrónico, servidor y otras aplicaciones.

8.4.1 Acceso a redes

8.4.1.1 Solo los equipos informáticos registrados (Desktops o Laptops) tienen capacidad para conectarse a la red.

8.4.1.2 El acceso a la red para el uso de los recursos y servicios informáticos se realizará con el uso de un usuario de red personal e intransferible.

8.4.1.3 La creación de un usuario debe ser solicitada por el Dpto. de Talento Humano con copia al jefe o encargado del área, vía correo electrónico.

8.4.1.4 Las contraseñas de red se crearán con un mínimo de **8** caracteres las mismas que deben estar formadas tanto por números, letras y caracteres especiales.

8.4.1.5 Los usuarios deben usar de manera obligatoria la doble autenticación mediante (Authenticator Microsoft).

8.4.1.6 Las contraseñas de Windows expirarán cada 2 meses de forma automática. Los usuarios deben colocar contraseñas nuevas no iguales a las anteriores.

8.4.1.7 Los usuarios podrán realizar 5 intentos de validación de su contraseña antes de bloquearse el usuario por seguridad.

8.4.1.8 Los accesos a recursos compartidos de red (carpetas compartidas) serán solicitadas por el jefe o encargado del área al Dpto. de TI, vía correo.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 5 de 13

8.4.2 Acceso al SAP y otras aplicaciones

8.4.2.1 El acceso a la información se realizará con el uso de un usuario de aplicación personal e intransferible.

8.4.2.2 La contraseña de usuario tendrá como mínimo de **8** caracteres, las mismas que deben estar formadas por números y letras.

8.4.2.3 Las contraseñas expirarán cada 3 meses de forma automática. Los usuarios deben colocar contraseñas nuevas no iguales a las anteriores.

8.4.2.4 Los usuarios podrán realizar 3 intentos de validación de su contraseña antes de bloquearse el usuario por seguridad.

8.4.2.5 Los accesos a opciones o información serán solicitados por el jefe o encargado del área al Dpto. de TI, vía correo electrónico.

8.4.2.6 Está prohibido cualquier manipulación de la información que no sea empleando los aplicativos desarrollados.

8.4.3 Del Acceso a Internet

8.4.3.1 La entrada o salida de información desde o hacia Internet pasa a través de un equipo de seguridad denominado firewall.

8.4.3.2 El acceso a Internet se ha restringido mediante un equipo firewall, solamente permite el acceso a páginas Web necesarias para la normal operatividad de la empresa.

8.4.3.3 Se realiza también, un filtro de seguridad para rechazar correos que puedan contener archivos adjuntos infectados por virus informáticos y archivos de gran capacidad (hasta 20 megabytes) a través de Security de 365.

8.4.3.4 En caso de visitantes, se les brinda acceso con un código de visitante.

8.4.3.5 Los accesos a Internet solo pueden ser autorizados por el jefe o encargado del área, vía correo electrónico. Solo en los casos que las funciones del empleado ameriten este acceso. En caso de que un usuario este haciendo uso no autorizado de este medio se informará a su superior para que tome las medidas o sanciones pertinentes.

8.4.3.6 Está prohibido el uso de cualquier programa para la navegación o comunicación que no haya sido instalado por el Dpto. de TI.

8.4.3.7 Se han definido grupos para la navegación en Internet:

8.4.3.7.1 Laboral: Grupo de usuarios estándar.

8.4.3.7.2 Especifico: Grupo de usuarios que solo ingresan a sitios limitados en Internet.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 6 de 13

8.4.3.7.3 Managers: Grupo conformado por los administradores de la red.

8.4.3.7.4 Servidores: Acceso de navegación para los servidores

8.4.3.7.5 Amenazas: Grupo que contiene los lugares en Internet que pueden atacar nuestra red.

8.4.4 Del Acceso a Llamadas Telefónicas

8.4.4.1 Los accesos para llamadas telefónicas deberán ser autorizadas por el jefe o encargado del área, vía correo electrónico.

8.4.4.2 En caso de asignación de un teléfono de la empresa con un plan corporativo este se debe utilizar para labores de la empresa.

8.4.4.3 Los tipos de planes que tendrá el usuario (llamadas locales, móviles, nacionales o internacionales) serán definidos por el jefe o encargado del área.

8.4.5 Acceso a VPN.

8.4.5.1 Dado que todos los programas, aplicativos son de acceso directo por el usuario por internet, no hay acceso por VPN.

8.4.5.2 Para el acceso a equipos por parte de usuarios desde un punto remoto, se realizará por soporte por aplicativos remotos adquiridos por PRODAC con sus respectivas licencias de uso y conformidad del departamento de TI.

8.5 Seguridad en los Sistemas Informáticos para los Usuarios

8.5.1 Equipos de Computo

8.5.1.1 Debe conservar en buen estado el equipo asignado. Evitando su deterioro.

8.5.1.2 No se debe instalar ningún tipo de Software. Toda instalación debe ser coordinada con el Dpto. de TI.

8.5.1.3 No se debe desinstalar ninguno de los programas del equipo sin la aprobación del Dpto. de TI.

8.5.1.4 Está prohibido manipular o modificar las propiedades y/o protocolos de comunicación de los equipos.

8.5.1.5 No colocar en el equipo USB, CD o Discos magnéticos que contengan información de dudosa procedencia. Si se desea hacer uso de estos recursos debe tener la autorización de su jefe dirigida al Dpto. de TI.

8.5.2 Uso de Internet

8.5.2.1 El uso de Internet es restringido, para tener acceso al mismo debe contar con la autorización de su jefe Inmediato dirigido al Dpto. de TI.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 7 de 13

8.5.2.2 De contar con Internet está prohibida la navegación en páginas o portales, que no sean con fines laborales sin excepción.

8.5.2.3 No se debe enviar información formal de la empresa a través de medios que no sean autorizados por el Dpto. de TI.

8.5.3 Uso del correo

8.5.3.1 El correo electrónico es de uso exclusivo para fines laborales.

8.5.3.2 No enviar por este medio archivos mayores a 20 Megabytes para ellos compartir vía SharePoint o OneDrive. Por tal motivo el aplicativo no le permitirá enviar correos que superen este tamaño.

8.5.4 Uso de claves telefónicas

8.5.4.1 La clave para llamadas telefónicas es de uso personal e intransferible.

8.5.4.2 El uso de este acceso es solo para llamadas de trabajo.

8.6 De la Seguridad en los Puertos de Entrada (USB)

8.6.1 Está terminantemente prohibido conectar dispositivos de almacenamiento con entrada USB en los computadores/Laptop a excepción de aquellos que la Gerencia Usuaría autorice en conjunto con el Dpto. de TI.

8.6.2 Para salvaguardar la información de la organización se han deshabilitado las entradas de los puertos USB para el almacenamiento de información.

8.7 De la Detección de Abusos a los Sistemas Informáticos

8.7.1 El software ERP SAP cuenta con una bitácora de cada usuario a fin de poder verificar las modificaciones, eliminaciones, adiciones y otros que este pueda realizar.

8.8 De la Sanciones a los Infractores por Incumplimiento al Procedimiento

8.8.1 De detectarse incumplimiento a las políticas de sistemas de información e informáticos, se determina la evaluación con Gerencia General y/o Gerencia Usuaría para las sanciones disciplinarias que

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 8 de 13

pueden alcanzar la desvinculación laboral y/o aplicación de sanciones legales de acuerdo con lo indicado en el **Reglamento Interno de Trabajo**.

8.8.2 El cumplimiento de las políticas de seguridad de la información e informático incluye los siguientes actos:

8.8.2.1 Exponga intencionalmente el equipo informático a un peligro de mal funcionamiento, degradación o falla permanente.

8.8.2.2 Deteriore o descomponga premeditadamente el equipo informático.

8.8.2.3 Intento a la vulnerabilidad a accesos no autorizados (Referenciar al reglamento interno).

Nro.	FALTA COMETIDA	OCURRENCIA		
		PRIMERA VEZ	SEGUNDA VEZ	TERCERA VEZ
1	Instalación de software no autorizado	Amonestación escrita	Suspensión temporal	Despido Laboral
2	Acceso a páginas de internet no permitidas	Amonestación escrita	Suspensión temporal	Despido Laboral
3	Mal uso de los equipos de computo	Amonestación escrita	Suspensión temporal	Despido Laboral
4	Perdida y robo de Celulares - Laptops	No aplica descuento	50% descuento del valor del equipo	100 % del Valor del equipo
5	Mal uso de los sistemas de información	Amonestación escrita	Suspensión temporal	Despido Laboral

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 9 de 13

8.8.3 Cualquier persona que tenga conocimiento del incumplimiento al procedimiento de Seguridad de la Información e Informático, debe reportarla inmediatamente al jefe inmediato superior o Gerente de área correspondiente quien, a su vez, debe comunicar al **Gerente** de TI.

8.9 Del Acceso al Software de Terceros

8.9.1 Para la operatividad integral de la empresa, se cuenta con softwares de terceros los mismo que ha sido adquiridos a un **proveedor de software**.

8.9.2 El **proveedor de software**, mediante contrato, se encarga de darle mantenimiento y actualización al software. Todo cambio a las aplicaciones es comunicado a fin de realizar la descarga de las actualizaciones en el servidor, siendo responsable el **Gerente de TI**.

8.10 De la Creación de Nuevos Usuarios

8.10.1 Para la creación y conexión de nuevos usuarios a la red, se sigue el presente procedimiento:

8.10.1.1 El Área de Talento Humano solicita la creación del **usuario** al **Gerente de TI** con copia al **jefe de Área o Gerente de Área**, a través de un correo, para dar la autorización.

8.10.1.2 Se crea y registra el **USUARIO**, que está conformado por el primer nombre y apellido.

8.10.1.3 De la Asignación de Accesos de acuerdo con la Solicitud Recibida.

8.10.1.4 El Gerente de cada área es quien asigna los accesos y atributos a los colaboradores de la organización de acuerdo con el puesto que ocupen, solicitando mediante correo al Gerente de TI que asigna los atributos y privilegios de accesos a los sistemas informáticos

8.11 De la asignación de roles y transacciones en SAP

8.11.1 El usuario que necesite el acceso a un rol o transacción deberá solicitar vía app de Helpdesk o correo electrónico con copia a su gerente o jefe inmediato.

8.11.2 El formulario deberá ser enviado a la gerencia de Ti con la aprobación de su jefe inmediato.

8.11.3 La gerencia de Ti se encargará de aprobar dicha solicitud para su ejecución.

8.11.4 Soporte técnico creara el usuario mediante el perfil designado al área solicitante.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 10 de 13

8.12 De la Baja de Usuarios

- 8.12.1** Mediante la notificación de correo electrónico que notifica el cese de colaboradores, soporte técnico toma acción para la baja del usuario.
- 8.12.2** La gerencia de TI dará de baja al usuario de todas las plataformas que tenga la compañía en un plazo de 48 horas.
- 8.12.3** La extensión de la cuenta del usuario deberá contar con la aprobación del gerente de área y la gerencia de sistemas por un plazo no mayor a 15 días.
- 8.12.4** El **Gerente de TI**, delega a soporte técnico el redireccionamiento de los correos al nuevo personal o a su jefe inmediato superior, por un periodo determinado.
- 8.12.5** Pasado el periodo, el Gerente de TI emite la orden de anular el usuario y el correo corporativo habiendo hecho el Backup de la información de este si fuese requerido.

8.13 De la Pantalla de Bloqueo

- 8.13.1** Todas las computadoras y laptop personales tienen activado el bloqueo de pantalla con contraseña de manera obligatoria.
- 8.13.2** Cada 15 minutos, de manera automática, se activa el bloqueo de pantalla cuando el usuario no utiliza el equipo de cómputo.
- 8.13.3** El personal al ausentarse de su sitio bloquea su pantalla presionando la tecla de Windows + L.  

8.14 Del Back Up. (Copia de seguridad)

- 8.14.1** El proceso de Backup cuenta con el instructivo **Backups (I-SIG-SIS-001)** en los cuales se detallan el proceso de las copias de respaldo de la información.

8.15 Control y Monitoreo

8.15.1 Revisión Recurrente

- 8.15.1.1** El Dpto. de TI realizará el monitoreo del cumplimiento según lo siguiente:
- 8.15.1.1.1** Revisión trimestral del contenido de las carpetas compartidas centralizadas.
- 8.15.1.1.2** Revisión anual física y lógica de las computadoras personales.
- 8.15.1.1.3** Revisión mensual de los accesos internet.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 11 de 13

8.15.1.1.4 Revisión semestral aleatoria de los accesos a la red interna.

8.15.1.2 En todos estos casos, se eliminarán los elementos de aplicación y de información que no son de propiedad de la Empresa.

8.15.2 Revisión No Programada

8.15.2.1 El Dpto. de TI realizará las verificaciones de contenido de los equipos cada vez que se realice un mantenimiento preventivo o correctivo, eliminando los elementos de aplicación y de información que no son de propiedad de la Empresa.

8.15.2.2 Los equipos del personal del Dpto. de TI serán revisados en forma aleatoria, al menos tres veces al año.

8.15.3 Reporte de hallazgos

8.15.3.1 Todas las irregularidades encontradas serán reportadas al jefe o gerente de área afectada, así como al Gerente de TI.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 12 de 13

8.16 Del Mantenimiento Preventivo

8.16.1 El Dpto. de Sistemas mantiene un **Cronograma de Mantenimiento Preventivo** para todos los equipos de Cómputo de la empresa, que se realiza cada 6 meses para equipos Críticos en Planta y anual para equipos administrativos, que es realizado por un proveedor externo.

8.17 De las Capacitaciones

8.17.1 Mediante las capacitaciones programadas una vez al año, se da a conocer la **Política de la seguridad de la información e informática** que tiene la organización, así como también de las infracciones / sanciones que puedan cometer los colaboradores.

8.17.2 Mediante correos masivos, el **Gerente de TI** informa sobre posibles peligros y refuerza acerca de los controles que deben cumplir de acuerdo con las políticas de la organización.

8.18 De la Contingencia

8.18.1 Ante una contingencia de la caída en los Servidores Críticos Locales NO SAP, se cuenta con la opción de reestablecer los servidores críticos mediante la herramienta de Backup para ello se debe realizar mediante el procedimiento de restore.

8.18.2 Ante una contingencia de la caída de los servicios SAP en IBM la Molina se procederá a utilizar el centro de cómputo de IBM en San Isidro a fin de que se pueda restablecer las operaciones teniendo un tiempo de 3 horas aproximadamente.

8.18.3 Ante una contingencia de la caída del fluido eléctrico en PRODAC S.A., se cuenta con un grupo electrógeno propio que restablece en no más de 30 minutos el fluido eléctrico en las áreas críticas. En el Data Center se cuenta con un sistema UPS que da 1 hora de autonomía.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS

	PROCEDIMIENTO	Código:	P-SIG-SIS-002
	SEGURIDAD DE LA INFORMACIÓN Y DEL SISTEMA INFORMATICO	Revisión:	01
		Fecha:	15 / 12 / 2023
		Página:	Página 13 de 13

9. REFERENCIAS/ANEXOS

No aplica



Manuel Gallofré Cassadó
Gerente General
Prodac S.A.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
KIMBERLEY RODRIGUEZ	LUIS RAYGADA	ROSE MARIE SALINI
ADMINISTRADOR DE REDES Y COMUNICACIONES	GERENTE DE TECNOLOGIA DE LA INFORMACION	GERENTE DE ADMINISTRACIÓN Y FINANZAS